

RANDOM NILPOTENT GROUPS I

MATTHEW CORDES[♣], MOON DUCHIN[◇], YEN DUONG[♡], MENG-CHE HO[♣],
AND ANDREW P. SÁNCHEZ[◇]

ABSTRACT. We study random nilpotent groups in the well-established style of random groups, by choosing relators uniformly among freely reduced words of (nearly) equal length and letting the length tend to infinity. Whereas random groups $\Gamma = F_m/\langle\langle R \rangle\rangle$ are quotients of a free group by such a random set of relators, *random nilpotent groups* are formed as corresponding quotients $G = N_{s,m}/\langle\langle R \rangle\rangle$ of a free nilpotent group.

Using arithmetic uniformity for the random walk on \mathbb{Z}^m and group-theoretic results relating a nilpotent group to its abelianization, we are able to deduce statements about the distribution of ranks for random nilpotent groups from the literature on random lattices and random matrices. We obtain results about the distribution of group orders for some finite-order cases as well as the probability that random nilpotent groups are abelian. For example, for balanced presentations (number of relators equal to number of generators), the probability that a random nilpotent group is abelian can be calculated for each rank m , and approaches 84.69...% as $m \rightarrow \infty$. Further, abelian implies cyclic in this setting (asymptotically almost surely).

Considering the abelianization also yields the precise vanishing threshold for random nilpotent groups—the analog of the famous density one-half theorem for random groups. A random nilpotent group is trivial if and only if the corresponding random group is *perfect*, i.e., is equal to its commutator subgroup, so this gives a precise threshold at which random groups are perfect. More generally, we describe how to lift results about random nilpotent groups to obtain information about the lower central series of standard random groups.

1. INTRODUCTION AND BACKGROUND

1.1. Random groups. The background idea for the paper is the models of random groups $\Gamma = F_m/\langle\langle R \rangle\rangle$, where F_m is the free group on some number m of generators, and R is a set of relators of length ℓ chosen by a random process. Typically one takes the number of relators $|R|$ to be a function of ℓ ; for fixed ℓ , there are finitely many choices of R of a certain size, and they are all made equally likely. For instance, in the *few-relators model*, $|R|$ is a fixed constant, and in the standard *density model*, $|R| = (2m-1)^{d\ell}$ for a density parameter $0 < d < 1$. (When the number of relators has sub-exponential growth, this is often regarded as sitting in the density model at density zero.)

After fixing $|R|$ as a function of ℓ , we can write $\Pr(\Gamma \text{ has property } P) = p$ to mean that the proportion of such presentations for which the group has P tends to p as $\ell \rightarrow \infty$. In particular, we say that random groups have P asymptotically almost surely (a.a.s.) if the probability tends to 1.

The central result in the study of random groups is the theorem of Gromov–Ollivier stating that for $d > 1/2$ in the density model, Γ is a.a.s. isomorphic to either $\{1\}$ or $\mathbb{Z}/2\mathbb{Z}$ (depending on the parity of ℓ), while for $d < 1/2$, Γ is a.a.s. non-elementary hyperbolic and torsion-free [12, Thm 11]. In the rest of this paper, we will choose our relators from those of length ℓ and $\ell-1$ with equal probability in order to avoid the parity issue; with this convention, $\Gamma \cong \{1\}$ a.a.s. for $d > 1/2$.

The Gromov–Ollivier theorem tells us that the density threshold for trivializing a free group coincides with the threshold for hyperbolicity, which means that one never sees other kinds of groups, for example abelian groups, in this model. Indeed, because \mathbb{Z}^2 can not appear as a subgroup of a hyperbolic group, one never sees a group with even one pair of commuting elements. To be precise, all finitely-generated groups are quotients of F_m , but probability of getting a nontrivial, non-hyperbolic

♣ TECHNION - IIT, Haifa, Israel, ◇ TUFTS UNIVERSITY, Medford MA, USA, ♡ UNIVERSITY OF ILLINOIS AT CHICAGO, Chicago IL, USA, ♣ UNIVERSITY OF WISCONSIN AT MADISON, Madison WI, USA
Correspondence: moon.duchin@tufts.edu.

group (or a group with torsion) is asymptotically zero at every density $d \neq 1/2$. Furthermore the recent paper [4] shows that this trivial/hyperbolic dichotomy seems to persist even at $d = 1/2$.

However, it is a simple matter to create new models of random groups by starting with a different “seed” group in place of the free group F_m . The r random strings in $\{a_1, \dots, a_m\}$ that are taken as relators in the Gromov model can be interpreted as elements of any other group with m generators. For instance, forming random quotients of the free abelian group \mathbb{Z}^m in this way would produce a model of random abelian groups; equivalently, the random groups arise as cokernels of random $m \times r$ integer matrices with columns given by the Gromov process, and these clearly recover the abelianizations of Gromov random groups. Random abelian groups are relatively well-studied, and information pertaining to their rank distribution can be found in at least three distinct places: the important paper of Dunfield–Thurston testing the virtual Haken conjecture through random models [5, §3.14]; the recent paper of Kravchenko–Mazur–Petrenko on generation of algebras by random elements [9]; and the preprint of Wang–Stanley on the Smith normal form distribution of random matrices [17]. These papers use notions of random matrices that differ from the one induced by the Gromov model, but we will explain some of the distinctions below. By contrast, there are many other ways that random abelian groups arise in mathematics: as class groups of imaginary quadratic fields, for instance, or as cokernels of graph Laplacians for random graphs (also known as *sandpile groups*). For a discussion of heuristics for these various distributions and a useful survey of some of the random abelian group literature, see [18] and its references.

In this paper we initiate a study of random nilpotent groups by beginning with the *free nilpotent group* $N_{s,m}$ of step s and rank m and adding random relators as above. Note that all nilpotent groups occur as quotients of appropriate $N_{s,m}$, just as all abelian groups are quotients of some \mathbb{Z}^m and all groups are quotients of some F_m (here and throughout, groups are taken to be finitely generated). By construction, these free nilpotent groups can be thought of as “nilpotentizations” of Gromov random groups; their abelianizations will agree with those described in the last paragraph (cokernels of random matrices), but they have a nontrivial lower central series and therefore retain more information about the original random groups.

Below, we begin to study the typical properties of random nilpotent groups. For instance, one would expect that the threshold for trivialization occurs with far fewer relators than for free groups, and also that nontrivial abelian quotients should occur with positive probability at some range of relator growth.

The results of this paper are summarized as follows:

- In the remainder of this section, we establish a sequence of group theory and linear algebra lemmas for the following parts.
- In §2, the properties of \mathbb{Z}^m random walk and its non-backtracking variant are described in order to deduce arithmetic statistics of Mal’cev coordinates.
- We survey the existing results from which ranks of random abelian groups can be calculated; a theorem of Magnus guarantees that the rank of a nilpotent group equals the rank of its abelianization. (§3)
- We give a complete description of one-relator quotients of the Heisenberg group, and compute the orders of finite quotients with any number of relators. (§4)
- Using a Freiheitssatz for nilpotent groups, we study the consequences of rank drop, and conclude that abelian groups occur with probability zero for $|R| \leq m - 2$, while they have positive probability for larger numbers of relators. Adding relators in a stochastic process drops the rank by at most one per new relator, with statistics for successive rank drop given by number-theoretic properties of the Mal’cev coordinates. (§5)
- We give a self-contained proof that a random nilpotent group is a.a.s. trivial exactly if $|R|$ is unbounded as a function of ℓ . We show how information about the nilpotent quotient lifts to information about the LCS of a standard (Gromov) random group and observe that standard random groups are *perfect* under the same conditions. (§6)

- Finally, the last section records experimental data gathered in Sage for random quotients of the Heisenberg group, showing in particular the variety of non-isomorphic groups visible in this model of random nilpotent groups and indicating some of their group-theoretic properties. (§7)

1.2. Nilpotent groups and Mal'cev coordinates. Nilpotent groups are those for which nested commutators become trivial after a certain uniform depth. We will adopt the commutator convention that $[a, b] = aba^{-1}b^{-1}$ and define nested commutators on the left by $[a, b, c] = [[a, b], c]$, $[a, b, c, d] = [[[a, b], c], d]$, and so on. Within a group we will write $[H, K]$ for the subgroup generated by all commutators $[h, k]$ with h ranging over $H \leq G$ and k ranging over $K \leq G$, so that in particular $[G, G]$ is the usual commutator subgroup of G . A group is *s-step nilpotent* if all commutators with $s + 1$ arguments are trivial, but not all those with s arguments are. (The step of nilpotency is also known as the *class* of nilpotency.) With this convention, a group is abelian if and only if it is one-step nilpotent. References for the basic theory of nilpotent groups are [16, Ch 9], [2, Ch 10-12].

In the free group F_m of rank m , let

$$T_{j,m} = \{[a_{i_1}, \dots, a_{i_j}] : 1 \leq i_1, \dots, i_j \leq m\}$$

be the set of all nested commutators with j arguments ranging over the generators. Then the *free s-step rank-m nilpotent group* is

$$N_{s,m} = F_m / \langle\langle T_{s+1,m} \rangle\rangle = \langle a_1, \dots, a_m \mid [a_{i_1}, \dots, a_{i_{s+1}}] \text{ for all } i_j \rangle,$$

where $\langle\langle R \rangle\rangle$ denotes the normal closure of a set R when its ambient group is understood. Just as all finitely-generated groups are quotients of (finite-rank) free groups, all finitely-generated nilpotent groups are quotients of free nilpotent groups. Note that the standard Heisenberg group $H(\mathbb{Z}) = \langle a, b \mid [a, b, a], [a, b, b] \rangle$ is realized as $N_{2,2}$. In the Heisenberg group, we will use the notation $c = [a, b]$, so that the center is $\langle c \rangle$.

The *lower central series* (LCS) for a s -step nilpotent group G is a sequence of subgroups inductively defined by $G_{k+1} = [G_k, G]$ which form a subnormal series

$$\{1\} = G_{s+1} \triangleleft \dots \triangleleft G_3 \triangleleft G_2 \triangleleft G_1 = G.$$

(The indexing is set up so that $[G_i, G_j] \subset G_{i+j}$.) For finitely generated nilpotent groups, this can always be refined to a *polycyclic series*

$$\{1\} = CG_{n+1} \triangleleft CG_n \triangleleft \dots \triangleleft CG_2 \triangleleft CG_1 = G$$

where each CG_i/CG_{i+1} is cyclic, so either \mathbb{Z} or $\mathbb{Z}/n_i\mathbb{Z}$. The number of \mathbb{Z} quotients in any polycyclic series for G is called the *Hirsch length* of G . From a polycyclic series we can form a generating set which supports a useful normal form for G . Make a choice of u_i in each CG_i so that $u_i CG_{i+1}$ generates CG_i/CG_{i+1} . An inductive argument shows that the set $\{u_1, \dots, u_n\}$ generates G . We call such a choice a *Mal'cev basis* for G , and we filter it as $MB_1 \sqcup \dots \sqcup MB_s$, with MB_j consisting of basis elements belonging to $G_j \setminus G_{j+1}$. Now if $u_i \in MB_j$, let τ_i be the smallest value such that $u_i^{\tau_i} \in MB_{j+1}$, putting $\tau_i = \infty$ if no such power exists. Then the Mal'cev normal form in G is as follows: every element $g \in G$ has a unique expression as $g = u_1^{t_1} \dots u_n^{t_n}$, with integer exponents and $0 \leq t_i \leq \tau_i$ if $\tau_i < \infty$. Then the tuple of exponents (t_1, \dots, t_n) gives a coordinate system on the group, called *Mal'cev coordinates*. We recall that $MB_j \sqcup \dots \sqcup MB_s$ generates G_j for each j and that (by definition of s) the elements of MB_s are central.

We will denote a Mal'cev basis for free nilpotent groups $N_{s,m}$ as follows: let $MB_1 = \{a_1, \dots, a_m\}$ be the basic generators, let $MB_2 = \{b_{ij} := [a_i, a_j] : i < j\}$ be the basic commutators, and take each MB_j as a subset of $T_{j,m}$ consisting of independent commutators from $[MB_{j-1}, MB_1]$. We note that $|MB_2| = \binom{m}{2}$, and more generally the orders are given by the *necklace polynomials*

$$|MB_j| = \frac{1}{j} \sum_{d|j} \mu(d) m^{j/d},$$

where μ is the Möbius function (see [7, Thm 11.2.2]).

For example, the Heisenberg group $H(\mathbb{Z}) = N_{2,2}$ has the lower central series $\{1\} \triangleleft \mathbb{Z} \triangleleft H(\mathbb{Z})$ with quotients \mathbb{Z} and \mathbb{Z}^2 , so its Hirsch length is 3. $H(\mathbb{Z})$ admits the Mal'cev basis a, b, c (with $a = a_1$, $b = a_2$, and c equal to their commutator), which supports a normal form $g = a^A b^B c^C$. The Mal'cev coordinates of a group element are the triple $(A, B, C) \in \mathbb{Z}^3$.

1.3. Group theory and linear algebra lemmas. In the free group $F_m = \langle a_1, \dots, a_m \rangle$, for any freely reduced $g \in F_m$, we define $A_i(g)$, called the *weight* of generator a_i in the word g , to be the exponent sum of a_i in g . Note that weights A_1, \dots, A_m are well defined in the same way for the free nilpotent group $N_{s,m}$ for any s . We will let ab be the abelianization map of a group, so that $\text{ab}(F_m) \cong \text{ab}(N_{s,m}) \cong \mathbb{Z}^m$. Under this isomorphism, we can identify $\text{ab}(g)$ with the vector $\mathbf{A}(g) := (A_1(g), \dots, A_m(g)) \in \mathbb{Z}^m$. If we have an automorphism ϕ on $N_{s,m}$, we write ϕ^{ab} for the induced map on \mathbb{Z}^m , which by construction satisfies $\text{ab} \circ \phi = \phi^{\text{ab}} \circ \text{ab}$. Note that $\mathbf{A}(g)$ is also the MB_1 part of the Mal'cev coordinates for g , and we can similarly define a b -weight vector $\mathbf{B}(g)$ to be the MB_2 part, recording the exponents of the b_{ij} in the normal form.

To fix terminology: the *rank* of any finitely-generated group will be the minimum size of any generating set. Note this is different from the *dimension* of an abelian group, which we define by $\dim(\mathbb{Z}^d \times G_0) = d$ for any finite group G_0 . (With this terminology, the Hirsch length of a nilpotent group G is the sum of the dimensions of its LCS quotients.) In any finitely-generated group, we say an element is *primitive* if it belongs to some basis (i.e., a generating set of minimum size). For a vector $w = (w_1, \dots, w_m) \in \mathbb{Z}^m$, we will write $\gcd(w)$ to denote the gcd of the entries. So a vector $w \in \mathbb{Z}^m$ is primitive iff $\gcd(w) = 1$. In this case we will say that the tuple (w_1, \dots, w_m) has the *relatively prime property* or is RP. As we will see below, an element $g \in N_{s,m}$ is primitive in that nilpotent group if and only if its abelianization is primitive in \mathbb{Z}^m , i.e., if $\mathbf{A}(g)$ is RP. In free groups, there *exists* a primitive element with the same abelianization as g iff $\mathbf{A}(g)$ is RP.

The latter follows from a classic theorem of Nielsen [11].

Theorem 1 (Nielsen primitivity theorem). For every relatively prime pair of integers (i, j) , there is a unique conjugacy class $[g]$ in the free group $F_2 = \langle a, b \rangle$ for which $A(g) = i$, $B(g) = j$, and g is primitive.

Corollary 2 (Primitivity criterion in free groups). There exists a primitive element $g \in F_m$ with $A_i(g) = w_i$ for $i = 1, \dots, m$ if and only if $\gcd(w_1, \dots, w_m) = 1$.

Proof. Let $w = (w_1, \dots, w_m)$. If $\gcd(w) \neq 1$, then the image of any g with those weights would not be primitive in the abelianization \mathbb{Z}^m , so no such g is primitive in F_m .

For the other direction we use induction on m , with the base case $m = 2$ established by Nielsen. Suppose there exists a primitive element of F_{m-1} with given weights w_1, \dots, w_{m-1} . For $\delta = \gcd(w_1, \dots, w_{m-1})$, we have $\gcd(\delta, w_m) = 1$. Let $\bar{w} = (\frac{w_1}{\delta}, \dots, \frac{w_{m-1}}{\delta})$. By the inductive hypothesis, there exists an element $\bar{g} \in F_{m-1}$ such that the weights of \bar{g} are \bar{w} , and \bar{g} can be extended to a basis $\{\bar{g}, h_2, \dots, h_{m-1}\}$ of F_{m-1} . Consider the free group $\langle \bar{g}, a_m \rangle \cong F_2$. Since $\gcd(\delta, w_m) = 1$, there exist \hat{g}, \hat{h} that generate this free group such that \hat{g} has weights $A_{\bar{g}}(\hat{g}) = \delta$ and $A_m(\hat{g}) = w_m$ by Nielsen. Consequently, $A_i(\hat{g}) = w_i$. Then $\langle \hat{g}, \hat{h}, h_2, \dots, h_{m-1} \rangle = \langle \bar{g}, h_2, \dots, h_{m-1}, a_m \rangle = F_m$, which shows that \hat{g} is primitive, as desired. \square

The criterion for primitivity in free nilpotent groups easily follows from a powerful theorem due to Magnus [10, Lem 5.9].

Theorem 3 (Magnus lifting theorem). If G is nilpotent and $S \subset G$ is any set of elements such that $\text{ab}(S)$ generates $\text{ab}(G)$, then S generates G .

Note that this implies that if G is nilpotent of rank m , then $G/\langle\langle g \rangle\rangle$ has rank at least $m - 1$, because we can drop at most one dimension in the abelianization.

Corollary 4 (Primitivity criterion in free nilpotent groups). An element $g \in N_{s,m}$ is primitive if and only if $\mathbf{A}(g)$ is primitive in \mathbb{Z}^m .

Now we establish a sequence of lemmas for working with rank and primitivity. Recall that a, b are the basic generators of the Heisenberg group $H(\mathbb{Z})$ and that $c = [a, b]$ is the central letter.

Lemma 5 (Heisenberg basis change). For any integers i, j , there is an automorphism ϕ of $H(\mathbb{Z}) = N_{2,2}$ such that $\phi(a^i b^j c^k) = b^d c^m$, where $d = \gcd(i, j)$ and $m = \frac{ij}{2d}(d-1) + k$.

In particular, if i, j are relatively prime, then there is an automorphism ϕ of $H(\mathbb{Z})$ such that $\phi(a^i b^j) = b$.

Proof. Suppose $ri + sj = d = \gcd(i, j)$ for integers r, s and consider $\hat{a} = a^s b^{-r}$, $\hat{b} = a^{i/d} b^{j/d}$. We compute

$$[a^s b^{-r}, a^{i/d} b^{j/d}] = [a^s, b^{j/d}] \cdot [b^{-r}, a^{i/d}] = c^{(ri+sj)/d} = c.$$

If we set $\hat{c} = c$, we have $[\hat{a}, \hat{b}] = \hat{c}$ and $[\hat{c}, \hat{a}] = [\hat{c}, \hat{b}] = 1$, so $\langle \hat{a}, \hat{b} \rangle$ presents a quotient of the Heisenberg group. We need to check that it is the full group. Consider $h = (\hat{a})^{-i/d} (\hat{b})^s$. Writing h in terms of a, b, c , the a -weight of h is 0 and the b -weight is $(ri + sj)/d = 1$, so $h = bc^t$ for some t . But then $b = (\hat{a})^{-i/d} (\hat{b})^s (\hat{c})^{-t}$ and similarly $a = (\hat{a})^{j/d} (\hat{b})^r (\hat{c})^{-t'}$ for some t' , so all of a, b, c can be expressed in terms of $\hat{a}, \hat{b}, \hat{c}$.

Finally,

$$(\hat{b})^d = (a^{i/d} b^{j/d})^d = a^i b^j c^{-\binom{d}{2} \frac{ij}{d^2}},$$

which gives the desired expression $a^i b^j c^k = (\hat{b})^d (\hat{c})^m$ from above. \square

Proposition 6 (General basis change). Let $\delta = \gcd(A_1(g), \dots, A_m(g))$ for any $g \in H = N_{s,m}$. Then there is an automorphism ϕ of H such that $\phi(g) = a_m^\delta \cdot h$ for some $h \in H_2$.

Proof. Let $w_i = A_i(g)$ for $i = 1, \dots, m$ and let $r_i = w_i/\delta$, so that $\gcd(r_1, \dots, r_m) = 1$. By Corollary 2, there exists a primitive element $x \in F_m$ with weights r_i . Let ϕ be a change of basis automorphism of F_m such that $\phi(x) = a_m$. This induces an automorphism of H , which we will also call ϕ .

By construction, x^δ and g have weight w . Since $\text{ab}(x^\delta) = \text{ab}(g) = w$, we must have $\phi^{\text{ab}}(w) = \text{ab}(\phi(x^\delta)) = \text{ab}(\phi(g))$. Therefore $\phi(x^\delta)$ and $\phi(g)$ have the same weights.

Then $\text{ab}(\phi(g)) = \text{ab}(\phi(x^\delta)) = \text{ab}(\phi(x)^\delta) = \text{ab}(a_m^\delta)$, so $\phi(g)$ and a_m^δ only differ by commutators, i.e., $\phi(g) = a_m^\delta \cdot h$ for some $h \in H_2$. \square

Remark 7. Given an abelian group $G = \mathbb{Z}^m / \langle R \rangle$, the classification of finitely-generated abelian groups provides that there are non-negative integers d_1, \dots, d_m with $d_m | d_{m-1} | \dots | d_1$ such that $G \cong \bigoplus_{i=1}^m \mathbb{Z}/d_i \mathbb{Z}$. If G has dimension q and rank r , then $d_1 = \dots = d_q = 0$, and $d_{r+1} = \dots = d_m = 1$, so that

$$G \cong \mathbb{Z}^q \times (\mathbb{Z}/d_{q+1} \mathbb{Z} \times \dots \times \mathbb{Z}/d_r \mathbb{Z}).$$

Now consider a projection map $f : \mathbb{Z}^m \rightarrow \mathbb{Z}^m / K \cong \bigoplus_{i=1}^m \mathbb{Z}/d_i \mathbb{Z}$. We can choose a basis e_1, \dots, e_m of \mathbb{Z}^m so that

$$K = \text{span}\{d_1 e_1, \dots, d_m e_m\} \cong \bigoplus_{i=1}^m d_i \mathbb{Z}.$$

Then since every element in K is a linear combination of $\{d_1 e_1, \dots, d_m e_m\}$ and $d_m | d_{m-1} | \dots | d_1$, we have that d_m divides all the coordinates of all the elements in K . Also $d_m e_m \in K$ with e_m being primitive.

Lemma 8 (Criterion for existence of primitive vector). Consider a set of r vectors in \mathbb{Z}^m , and let d be the gcd of the rm coordinate entries. Then there exists a vector in the span such that the gcd of its entries is d , and this is minimal among all vectors in the span.

In particular, a set of r vectors in \mathbb{Z}^m has a primitive vector in its span if and only if the gcd of the rm coordinate entries is 1.

Proof. With d as above, let K be the \mathbb{Z} -span of the vectors and let

$$\gamma := \inf_{w \in K} \gcd(w).$$

One direction is clear: every vector in the span has every coordinate divisible by d , so $\gamma \geq d$. On the other hand $d_m e_m \in K$ and $\gcd(d_m e_m) = d_m$ because e_m is primitive. But d_m is a common divisor of all rm coordinates, and d is the greatest such, so $d_m \leq d$ and thus $\gamma \leq d$. \square

Lemma 9 (Killing a primitive element). Let $H = N_{s,m}$ and let K be a normal subgroup of H . If $\text{rank}(H/K) < m$ then K contains a primitive element.

Proof. Since $\text{rank}(H/K) < m$, we also have $\text{rank}(\text{ab}(H/K)) < m$. Writing $\text{ab}(H/K) \cong \bigoplus_{i=1}^m \mathbb{Z}/d_i\mathbb{Z}$ as above, we have $d_m = 1$. By the previous lemma there is a primitive element in the kernel of the projection $\text{ab}(H) \rightarrow \text{ab}(H/K)$, and any preimage in K is still primitive (see Cor 4). \square

Lemma 10 (Linear algebra lemma). Suppose $u_1, \dots, u_n \in \mathbb{Z}^m$ and suppose there exists a primitive vector v in their span. Then there exist v_2, \dots, v_n such that $\text{span}(v, v_2, \dots, v_n) = \text{span}(u_1, \dots, u_n)$.

Proof. Since $v \in \text{span}(u_1, \dots, u_n)$, we can write $v = \alpha_1 u_1 + \dots + \alpha_n u_n$. Let $x \in \mathbb{Z}^n$ be the vector with coordinates α_i . Because $\gcd(v) = 1$, we have $\gcd(\alpha_i) = 1$, so x is primitive. Thus, we can complete x

to a basis of \mathbb{Z}^n , say $\{x, x_2, \dots, x_n\}$. Then take $\begin{pmatrix} -v- \\ -v_2- \\ \vdots \\ -v_n- \end{pmatrix} = \begin{pmatrix} -x- \\ -x_2- \\ \vdots \\ -x_n- \end{pmatrix} \cdot \begin{pmatrix} -u_1- \\ -u_2- \\ \vdots \\ -u_n- \end{pmatrix}$. Since $\begin{pmatrix} -x- \\ -x_2- \\ \vdots \\ -x_n- \end{pmatrix} \in$

$SL_n(\mathbb{Z})$, it represents a change of basis matrix, so we have $\text{span}(v, v_2, \dots, v_n) = \text{span}(u_1, \dots, u_n)$, as needed. \square

Lemma 11 (String arithmetic). Fix a free group $F = F_m$ on m generators and let R, S be arbitrary subsets, with normal closures $\langle\langle R \rangle\rangle, \langle\langle S \rangle\rangle$. Let $\phi : F \rightarrow F/\langle\langle R \rangle\rangle$ and $\psi : F \rightarrow F/\langle\langle S \rangle\rangle$ be the quotient homomorphisms. Then there exist canonical isomorphisms

$$(F/\langle\langle R \rangle\rangle)/\langle\langle \phi(S) \rangle\rangle \cong F/\langle\langle R \cup S \rangle\rangle \cong (F/\langle\langle S \rangle\rangle)/\langle\langle \psi(R) \rangle\rangle$$

that are compatible with the underlying presentation (i.e., the projections from F commute with these isomorphisms).

Proof. We will abuse notation by writing strings from F and interpreting them in the various quotients we are considering. Then if $G = \langle F \mid T \rangle \cong F/\langle\langle T \rangle\rangle$ is a quotient of F and U is a subset of F , we can write $\langle G \mid U \rangle$ to mean $F/\langle\langle T \cup U \rangle\rangle$ and can equally well write $\langle F \mid T, U \rangle$. Then the isomorphisms we need just record the fact that

$$\langle F \mid R, S \rangle = \langle F/\langle\langle R \rangle\rangle \mid S \rangle = \langle F/\langle\langle S \rangle\rangle \mid R \rangle. \quad \square$$

Because of this standard abuse of notation where we will variously interpret a string in $\{a_1, \dots, a_m\}^\pm$ as belonging to F_m , $N_{s,m}$, or some other quotient group, we will use the symbol $=_G$ to denote equality in the group G when trying to emphasize the appropriate ambient group.

2. RANDOM WALK AND ARITHMETIC UNIFORMITY

In this section we record some properties of the simple nearest-neighbor random walk (SRW) and the non-backtracking random walk (NBSRW) on the integer lattice \mathbb{Z}^m , then deduce consequences for the distribution of Mal'cev coordinates for random relators in free nilpotent groups. (See the Appendix for additional details [3].) For the standard basis $\{e_i\}$ of \mathbb{Z}^m , SRW is defined by giving the steps $\pm e_i$ equal probability $1/2m$, and NBSRW is similarly defined but with the added condition that the step $\pm e_i$ cannot be immediately followed by the step $\mp e_i$ (that is, a step can't undo the immediately previous step; equivalently, the position after k steps cannot equal the position after $k+2$ steps). A random string w_ℓ of ℓ letters from $\{a_1, \dots, a_m\}^\pm$ has the form $w_\ell = \alpha_1 \alpha_2 \dots \alpha_\ell$, where the α_i are i.i.d. random variables which equal each basic generator or its inverse with equal probability $1/2m$. The abelianization $X_\ell = \mathbf{A}(w_\ell)$ is a \mathbb{Z}^m -valued random variable corresponding to ℓ -step SRW. A random freely reduced string does not have an expression as a product of variables identically distributed under the same law, but if v_ℓ is such a string, its weight vector $Y_\ell = \mathbf{A}(v_\ell)$ is another \mathbb{Z}^m -valued random variable, this time corresponding to NBSRW.

It is well known that the distribution of endpoints for a simple random walk in \mathbb{Z}^m converges to a multivariate Gaussian: if X_ℓ is again the random variable recording the endpoint after ℓ steps of

simple random walk on \mathbb{Z}^m , and δ_t is the dilation in \mathbb{R}^m sending $v \mapsto tv$, we have the central limit theorem:

$$\delta_{\frac{1}{\sqrt{\ell}}} X_\ell \longrightarrow \mathcal{N}(\mathbf{0}, \frac{1}{m} I).$$

This convergence notation for a vector-valued random variable V_ℓ and a multivariate normal $\mathcal{N}(\mu, \Sigma)$ means that V_ℓ converges in distribution to $AW + \mu$, where the vector μ is the mean, $\Sigma = AA^T$ is the covariance matrix, and W is a vector-valued random variable with i.i.d. entries drawn from a standard (univariate) Gaussian distribution $\mathcal{N}(0, 1)$. In other words, this central limit theorem tells us that the individual entries of X_ℓ are asymptotically independent, Gaussian random variables with mean zero and expected magnitude $\sqrt{\ell}/m$. This is a special case of a much more general result of Wehn for Lie groups and can be found for instance in [1, Thm 1.3]. Fitzner and van der Hofstad derived a corresponding central limit theorem for NBSRW in [6]. Letting Y_ℓ be the \mathbb{Z}^m -valued random variable for ℓ -step NBSRW as before, they find that for $m \geq 2$,

$$\delta_{\frac{1}{\sqrt{\ell}}} Y_\ell \longrightarrow \mathcal{N}(\mathbf{0}, \frac{1}{m-1} I).$$

Note that the difference between the two statements records something intuitive: the non-backtracking walk still has mean zero, but the rule causes the expected size of the coordinates to be slightly higher than in the simple case; also, it blows up (as it should) in the case $m = 1$.

The setting of nilpotent groups is also well studied. To state the central limit theorem for free nilpotent groups, we take δ_t to be the similarity which scales each coordinate from MB_j by t^j , so that for instance in the Heisenberg group, $\delta_t(x, y, z) = (tx, ty, t^2z)$.

Proposition 12 (Distribution of Mal'cev coordinates). Suppose NB_ℓ is an $N_{s,m}$ -valued random variable chosen by non-backtracking simple random walk (NBSRW) on $\{a_1, \dots, a_m\}^\pm$ for ℓ steps. Then the distribution on the Mal'cev coordinates is asymptotically normal:

$$\delta_{\frac{1}{\sqrt{\ell}}} NB_\ell \sim \mathcal{N}(\mathbf{0}, \Sigma).$$

For SRW, this is called a “simple corollary” of Wehn’s theorem in [1, Thm 3.11]), where the only hypotheses are that the steps of the random walk are i.i.d. under a probability measure on $N_{s,m}$ that is centered, with finite second moment (in this case, the measure has finite support, so all moments are finite). Each Mal'cev coordinate is given by a polynomial formula in the a -weights of the variables α_i (the polynomial for an MB_j coordinate has degree j —for instance in $H(\mathbb{Z}) = N_{2,2}$ the coordinate C is a quadratic in $\mathbf{A}(\alpha_i)$). The number of summands in the polynomial gets large as $\ell \rightarrow \infty$. Switching to NBSRW, it is still the case that NB_ℓ is a product of group elements whose a -weight vectors are independent and normally distributed, so their images under the same polynomials will be normally distributed as well, with only the covariance differing from the SRW case. We sketch a simple and self-contained argument for this in the $N_{2,2}$ non-backtracking case—that the third Mal'cev coordinate in $H(\mathbb{Z})$ is normally distributed—which we note is easily generalizable to the other $N_{s,m}$ with (only) considerable notational suffering. Without loss of generality, the sample path of the random walk is

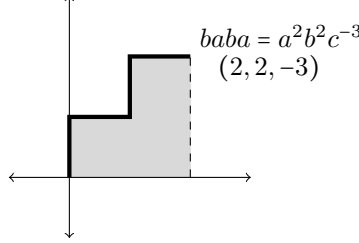
$$g = a^{i_1} b^{j_1} a^{i_2} b^{j_2} \dots a^{i_r} b^{j_r}$$

for some integers i_s, j_t summing to ℓ or $\ell - 1$, with all but possibly i_1 and j_r nonzero. After a certain number of steps, suppose the last letter so far was a . Then the next letter is either a , b , or b^{-1} with equal probability, so there is a $1/3$ chance of repeating the same letter and a $2/3$ chance of switching. This means that the i_s and j_t are (asymptotically independent) run-lengths of heads for a biased coin (Bernoulli trial) which lands heads with probability $1/3$. On the other hand, r is half the number of tails flipped by that coin in ℓ (or $\ell - 1$) trials. In Mal'cev normal form,

$$g = a^{\sum i_s} b^{\sum j_t} c^{\sum_{t < s} i_s j_t}.$$

Thus the exponent of c is obtained by adding products of run-lengths together $\binom{r}{2}$ times, and general central limit theorems ensure that adding many independent and identically distributed (i.i.d.) random variables together tends to a normal distribution.

Our distribution statement has a particularly nice formulation in this Heisenberg case, where the third Mal'cev coordinate records the *signed area* enclosed between the x -axis and the path traced out by a word in $\{a, b\}^\pm$. For instance, in the figure below, *baba* encloses area -3 , which equals the c exponent in the normal form.



Corollary 13 (Area interpretation for Heisenberg case). For the simple random walk on the plane, the signed area enclosed by the path is a normally distributed random variable.

Next, we want to describe the effect of a group automorphism on the distribution of coordinates. Then we conclude this section by considering the distribution of coordinates in various $\mathbb{Z}/p\mathbb{Z}$.

Corollary 14 (Distributions induced by automorphisms). If ϕ is an automorphism of $N_{s,m}$ and g is a random freely reduced word of length ℓ in $\{a_1, \dots, a_m\}^\pm$, then the Mal'cev coordinates of $\text{ab}(\phi(g))$ are also normally distributed.

Proof. The automorphism ϕ induces a change of basis on the copy of \mathbb{Z}^m in the MB_1 coordinates, which is given by left-multiplication by a matrix $B \in \text{SL}_m(\mathbb{Z})$. Then $\phi_*(Y_\ell) \rightarrow \mathcal{N}(\mathbf{0}, B\Sigma B^T)$. \square

Note that normality of the MB_j coordinates follows as well, as before: they are still described by sums of statistics coming from asymptotically independent Bernoulli trials, and only the coin bias has changed.

Relative primality of MB_1 coefficients turns out to be the key to studying the rank of quotient groups, so we will need some arithmetic lemmas.

Lemma 15 (Arithmetic uniformity). Let $A_{\ell,i}$ be the \mathbb{Z} -valued random variable given by the a_i -weight of a random word of length ℓ in $\{a_1, \dots, a_m\}^\pm$, for $1 \leq i \leq m$. Let $\hat{A}_{\ell,i}$ equal $A_{\ell,i}$ with probability $\frac{1}{2}$ and $A_{\ell-1,i}$ with probability $\frac{1}{2}$. Then $\forall \epsilon > 0 \quad \exists c_1, c_2 > 0$ s.t.

$$\forall n \leq \ell^{\frac{1}{2}-\epsilon}, \quad \forall k, \quad \Pr(\hat{A}_{\ell,i} \equiv k \pmod{n}) < \frac{1}{n} + c_1 e^{-c_2 \ell^{2\epsilon}}.$$

More generally $\exists c_1, c_2 > 0$ s.t. for any $s \leq m$ and distinct i_1, \dots, i_s ,

$$\forall n \leq \ell^{\frac{1}{2}-\epsilon}, \quad \forall k_1, \dots, k_s, \quad \Pr(\hat{A}_{\ell,i_1} \equiv k_1, \dots, \hat{A}_{\ell,i_s} \equiv k_s \pmod{n}) < \frac{1}{n^s} + c_1 e^{-c_2 \ell^{2\epsilon}}.$$

In other words, the $\mathbb{Z}/n\mathbb{Z}$ -valued random variables induced by the coordinate projections from random walk on the Mal'cev generators MB_1 approach independent uniform distributions.

Proof. Depending on whether the random word is chosen as a random string or a random freely reduced string, $A_{\ell,i}$ is the i th coordinate projection of either the SRW X_ℓ or the NBSRW Y_ℓ , and $\hat{A}_{\ell,i}$ is the parity-corrected version. We first consider the residues mod n for simple random walk X_ℓ on \mathbb{Z}^m by studying its position on the discrete torus $(\mathbb{Z}/n\mathbb{Z})^m$. We only need to consider the statement for s coordinates in the case $s = m$, since the results for $s < m$ can be derived from this by summing: for instance, the positions satisfying $\pi_i(X_\ell) \equiv k_i$ for $i = 1, 2$ are represented by n^{m-2} positions in the torus, so the bound can be added polynomially many times to get the right main term, at the cost of slightly enlarging the constant c_2 .

A theorem from Saloff-Coste [15, Theorem 7.8] controls the distance from a lazy symmetric generating random walk to the uniform distribution on any family of finite Cayley graphs which satisfies a uniform doubling bound on volume growth. (In our case, the growth $\#B_r$ is bounded on $(\mathbb{Z}/n\mathbb{Z})^m$

by $(2r+1)^m$, independent of n , and the graphs satisfy the doubling hypothesis.) First we will explain how this theorem provides the needed bound, then we will explain how to modify our random walk to satisfy the theorem's hypotheses.

In our notation, the theorem says that

$$\Pr(\pi_1(X_\ell) \equiv k_1, \dots, \pi_m(X_\ell) \equiv k_m \pmod n) < \frac{1}{n^m} + \frac{c_1 \cdot n^m}{\ell^{m/2}} e^{-c_2 \ell / (mn)^2},$$

for the following reasons: the L^2 distance upper-bounds the difference in probabilities at any single point, and the diameter of $(\mathbb{Z}/n\mathbb{Z})^m$ is less than mn . Since $n < \ell^{\frac{1}{2}-\epsilon}$, we have $n^2 < \ell^{1-2\epsilon}$, and by enlarging the constants we obtain

$$\Pr(\pi_1(X_\ell) \equiv k_1, \dots, \pi_m(X_\ell) \equiv k_m \pmod n) < \frac{1}{n^m} + c_1 e^{-c_2 \ell^{2\epsilon}},$$

as desired.

In order to use this theorem on our (non-lazy) walk, we apply the following technique: we replace the simple random walk P with the two-step walk $P * P$ which is lazy and symmetric. If n is odd, the support of $P * P$ is a generating set, and we can proceed. If n is even, $P * P$ is supported on the sublattice of torus points where the sum of the coordinates is even, which does not generate. But in that case the random variable \hat{A}_ℓ that we are studying (which takes either ℓ or $\ell-1$ steps) lives on the even or odd sublattice with equal probability; Saloff-Coste's statement will ensure equidistribution on the even sublattice, and by symmetry, taking one more step will equidistribute on the odds. (To be precise, we should use $\ell/2$ rather than ℓ on the right-hand side because of the parity fix, but this gets absorbed in the constants.)

To handle NBSRW, we can construct a new state space whose states correspond to directed edges on the discrete torus; this encodes the one step of memory required to avoid backtracking. This new state space can itself be rendered as a homogeneous finite graph, and a similar argument can be applied. \square

Corollary 16 (Uniformity mod p). The abelianization of a random freely reduced word in F_m has entries that are asymptotically uniformly distributed in $\mathbb{Z}/p\mathbb{Z}$ for each prime p , and the distribution mod p is asymptotically independent of the distribution mod q for any distinct primes p, q .

Proof. For independence, consider $n = pq$ in the previous Lemma. Asymptotically uniform implies asymptotically independent. \square

Corollary 17 (Probability of primitivity). For a random freely reduced word in F_m , the probability that it is primitive in abelianization tends to $1/\zeta(m)$, where ζ is the Riemann zeta function. In particular, for $m = 2$, the probability is $6/\pi^2$.

Proof. Using arithmetic uniformity, one derives a probability expression that agrees with $1/\zeta(m)$ by Euler's product formula for the zeta function, as in [8]. For details, see the Appendix [3]. \square

Remark 18 (Comparison of random models). As we have seen, abelianizations of Gromov random groups are computed as cokernels of random matrices M whose columns are given by non-backtracking simple random walk on \mathbb{Z}^m . Most other models in the random abelian groups literature use somewhat different randomization set-ups. Dunfield and Thurston [5] use a lazy random walk: ℓ letters are chosen uniformly from the $(2m+1)$ possibilities of a_i^\pm and the identity letter, creating a word of length $\leq \ell$, whose abelianization becomes a column of M . Results by Kravchenko–Mazur–Petrenko [9] and Wang–Stanley [17] use the standard “box” model: integer entries are drawn uniformly at random from $[-\ell, \ell]$, and asymptotics are calculated as $\ell \rightarrow \infty$. (This is the most classical way to randomize integers in number theory; see [8].)

However, the main arguments in each of these settings rely on arithmetic uniformity of coordinates mod p to calculate probabilities of relative primality, which is why the Riemann zeta function comes up repeatedly in the calculations.

3. PRELIMINARY FACTS ABOUT RANDOM NILPOTENT GROUPS VIA ABELIANIZATION

In this section we make a few observations relevant to the model of random nilpotent groups we study below. In particular, there has been substantial work on quotients of free abelian groups \mathbb{Z}^m by random lattices, so it is important to understand the relationship between a random nilpotent group and its abelianization. Below, and throughout the paper, recall that probabilities are asymptotic as $\ell \rightarrow \infty$.

First, we record the simple observation that depth in the LCS is respected by homomorphisms.

Lemma 19. Let $\phi : G \rightarrow H$ be a surjective group homomorphism. Then $\phi(G_k) = H_k$ where G_k, H_k are the level- k subgroups in the respective lower central series.

Proof. Since ϕ is a homomorphism, depth- k commutators are mapped to depth- k commutators, i.e., $\phi(G_k) \subseteq H_k$. Let $h \in H_k$. Without loss of generality we can assume h is a single nested commutator $h = [w_1, \dots, w_k]$. By surjectivity of ϕ we can choose lifts $\overline{w}_1, \dots, \overline{w}_k$ of w_1, \dots, w_k . We see $[\overline{w}_1, \dots, \overline{w}_k] \in G_k$ and $\phi(G_k) \supseteq H_k$. \square

To begin the consideration of ranks of random nilpotent groups, note that the Magnus lifting theorem (Theorem 3) tells us the rank of $N_{s,m}/\langle\langle R \rangle\rangle$ equals the rank of its abelianization $\mathbb{Z}^m/\langle R \rangle$, so we quickly deduce the probability of rank drop.

Proposition 20 (Rank drop). For a random r -relator nilpotent group $G = N_{s,m}/\langle\langle g_1, \dots, g_r \rangle\rangle$,

$$\Pr(\text{rank}(G) < m) = \frac{1}{\zeta(rm)}.$$

Proof. This follows directly from considering the existence of a primitive element in $\langle \text{ab}(R) \rangle$. By Lemma 8, this occurs if and only if the rm entries are relatively prime, and by arithmetic uniformity (Lemma 15), this is computed by the Riemann zeta function, as in Corollary 17. \square

Next we observe that a nilpotent group is trivial if and only if its abelianization (i.e., the corresponding \mathbb{Z}^m quotient) is trivial, and more generally it is finite if and only if the abelianization is finite. Equivalence of triviality follows directly from the Magnus lifting theorem (Theorem 3). For the other claim, suppose the abelianization is finite. Then powers of all the images of a_i are trivial in the abelianization, so in the nilpotent group G there are finite powers $a_i^{r_i}$ in the commutator subgroup G_2 . A simple inductive argument shows that every element of G_j has a finite power in G_{j+1} ; for example, consider $b_{ij} \in G_2$. Since $[a_i^{r_i}, a_j] = b_{ij}^{r_i}$ is a commutator of elements from G_2 and G_1 , it must be in G_3 , as claimed. But then we can see that there are only finitely many distinct elements in the group by considering the Mal'cev normal form

$$g = u_1^* u_2^* \dots u_r^*$$

and noting that each exponent can take only finitely many values. Since the rank of a nilpotent group equals that of its abelianization (by Theorem 3 again), it is also true that a nilpotent group is cyclic if and only if its abelianization is cyclic.

We introduce the term *balanced* for groups presented with the number of relators equal to the number of generators, so that it applies to models of random groups $F_m/\langle\langle R \rangle\rangle$, random nilpotent groups $N_{s,m}/\langle\langle R \rangle\rangle$, or random abelian groups $\mathbb{Z}^m/\langle R \rangle$, where $|R| = m$, the rank of the seed group. We will correspondingly use the terms *nearly-balanced* for $|R| = m - 1$, and *underbalanced* or *overbalanced* in the $|R| < m - 1$ and $|R| > m$ cases, respectively.

Then it is very easy to see that nearly-balanced (and thus underbalanced) groups are a.a.s. infinite, while balanced (and thus overbalanced) groups are a.a.s. finite because m random integer vectors (in any of the models) are \mathbb{R} -linearly independent with probability one. However, it is also easy to see that if $|R|$ is held constant, no matter how large, then there is a nonzero probability that the group is nontrivial (because, for example, all the a -weights could be even).

To set up the statement of the next lemma, let $Z(m) := \zeta(2) \dots \zeta(m)$ and

$$P(m) := \prod_{\text{primes } p} \left(1 + \frac{1/p - 1/p^m}{p - 1} \right).$$

As in Remark 18, we can quote the distribution results of [5],[9],[17] because of the common feature of arithmetic uniformity.

Lemma 21 (Cyclic quotients of abelian groups). The probability that the quotient of \mathbb{Z}^m by $m-1$ random vectors is cyclic is $1/Z(m)$. With m random vectors, the probability is $P(m)/Z(m)$.

These facts, particularly the first, can readily be derived “by hand,” but can also be computed using Dunfield–Thurston [5] as follows: their generating functions give expressions for the probability that i random vectors with $\mathbb{Z}/p\mathbb{Z}$ entries generate a subgroup of rank j , and the product over primes of the probability that the $\mathbb{Z}/p\mathbb{Z}$ reduction has rank $\geq m-1$ produces the probability of a cyclic quotient over \mathbb{Z} .

The latter fact appears directly in Wang–Stanley [17] as Theorem 4.9(i). We note that corresponding facts for higher-rank quotients could also be derived from either of these two papers, but the expressions have successively less succinct forms.

Corollary 22 (Explicit probabilities for cyclic quotients). For balanced and nearly-balanced presentations, the probability that a random abelian group or a random nilpotent group is cyclic is a strictly decreasing function of m which converges as $m \rightarrow \infty$.

In the balanced case, the limiting value is a well-known number-theoretic invariant. Values are estimated in the table below.

The convergence for both cases is proved in [17, Thm 4.9] as a corollary of the more general statement about the Smith normal form of a random not-necessarily-square matrix M , which is an expression $A = SMT$ for invertible S, T in which A has all zero entries except possibly its diagonal entries $a_{ii} = \alpha_i$. These α_i are then the abelian invariants for the quotient of \mathbb{Z}^m by the column span of M (that is, they are the d_i from Remark 7 but with opposite indexing, $d_i = \alpha_{m+1-i}$). The rank of the quotient is the number of these that are not equal to 1.

The probabilities of cyclic groups among balanced and nearly-balanced quotients of free abelian groups and therefore also for random nilpotent groups are approximated below. Values in the table are truncated (not rounded) at four digits.

Pr(cyclic)	$m = 2$	$m = 3$	$m = 4$	$m = 10$	$m = 100$	$m = 1000$	$m \rightarrow \infty$
$ R = m - 1$.6079	.5057	.4672	.4361	.4357	.4357	.4357
$ R = m$.9239	.8842	.8651	.8469	.8469	.8469	.8469

Computing the probability of a trivial quotient with r relators is equivalent to the the probability that r random vectors generate \mathbb{Z}^m .

Lemma 23 (Explicit probability of trivial quotients). For $r > m$,

$$\Pr\left(\mathbb{Z}^m / \langle v_1, \dots, v_r \rangle = 0\right) = \frac{1}{\zeta(r-m+1) \cdots \zeta(r)}.$$

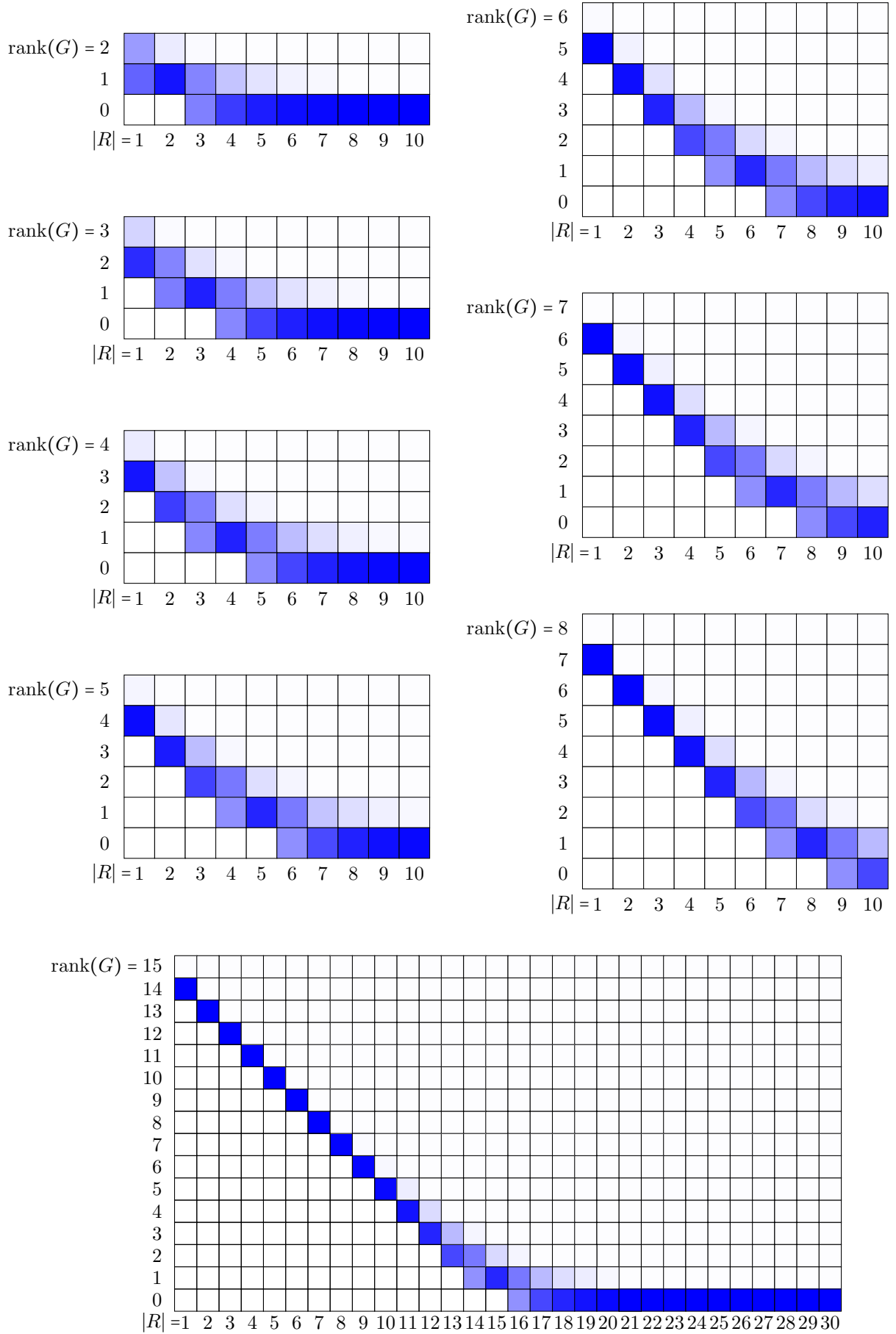
This is a rephrasing of [9, Cor 3.6] and [17, Thm 4.8].

Remark 24. From the description of Smith normal form, we get a symmetry in r and m , namely

$$\Pr\left(\text{rank}\left(\mathbb{Z}^m / \langle v_1, \dots, v_r \rangle\right) = m - k\right) = \Pr\left(\text{rank}\left(\mathbb{Z}^r / \langle v_1, \dots, v_m \rangle\right) = r - k\right) \quad \forall 1 \leq k \leq \min(r, m)$$

just by the observation that the transpose of the normal form expression has the same invariants. For example, applying duality to Lemma 21 and reindexing, we immediately obtain, as in Lemma 23,

$$\Pr\left(\mathbb{Z}^m / \langle v_1, \dots, v_{m+1} \rangle = 0\right) = \frac{1}{Z(m+1)} = \frac{1}{\zeta(2) \cdots \zeta(m+1)}.$$

FIGURE 1. The empirical distribution of ranks in $\mathbb{Z}^m / \langle R \rangle$ for $m = 2, 3, 4, 5, 6, 7, 8, 15$.

4. QUOTIENTS OF THE HEISENBERG GROUP

We will classify all $G := H(\mathbb{Z})/\langle\langle g \rangle\rangle$ for single relators g , up to isomorphism. As above, we write a, b for the generators of $H(\mathbb{Z})$, and $c = [a, b]$. With this notation, $H(\mathbb{Z})$ can be written as a semidirect product $\mathbb{Z}^2 \rtimes \mathbb{Z}$ via $\langle b, c \rangle \rtimes \langle a \rangle$ with the action of \mathbb{Z} on \mathbb{Z}^2 given by $ba = abc^{-1}$, $ca = ac$.

Theorem 25 (Classification of one-relator Heisenberg quotients). Suppose $g = a^i b^j c^k \neq 1$. Let $d = \gcd(i, j)$, let $m = \frac{ij}{2d}(d-1) + k$ as in Lemma 5, and let $D = \gcd(d, m)$. Then

$$G := H(\mathbb{Z})/\langle\langle g \rangle\rangle \cong \begin{cases} (\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}) \rtimes \mathbb{Z}, & \text{if } i = j = 0; \\ (\mathbb{Z}/\frac{d^2}{D}\mathbb{Z} \times \mathbb{Z}/D\mathbb{Z}) \rtimes \mathbb{Z}, & \text{else,} \end{cases}$$

with the convention that $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ and $\mathbb{Z}/1\mathbb{Z} = \{1\}$. In particular, G is abelian if and only if $g = c^{\pm 1}$ or $\gcd(i, j) = 1$; otherwise, it has step two. Furthermore, unless g is a power of c (the $i = j = 0$ case), the quotient group is virtually cyclic.

Note that this theorem is exact, not probabilistic.

Remark 26 (Baumslag-Solitar case). The *Baumslag-Solitar groups* are a famous class of groups given by the presentations $BS(p, q) = \langle a, b \mid ab^p a^{-1} = b^q \rangle$ for various p, q . For the Heisenberg quotients as described above, we will refer to $D = 1$ as the Baumslag-Solitar case, because in that case $sd - tm = 1$ has solutions in s, t , and one easily checks that the group is presented as

$$G = \langle a, b \mid [a, b] = b^{td}, \quad b^{d^2} = 1 \rangle \cong BS(1, 1 + td) / \langle\langle b^{d^2} \rangle\rangle,$$

a 1-relator quotient of a solvable Baumslag-Solitar group $BS(1, q)$.

Examples:

- (1) if $g = a$, then $G = \mathbb{Z}$.
- (2) if $g = c$, then $G = \mathbb{Z}^2$.
- (3) if $g = c^2$, then $G = (\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}$.
- (4) if $g = a^{20} b^{28} c^{16}$, we have $d = 4$, $m = 226$, $D = 2$, so we get

$$G = \left(\mathbb{Z}^2 / \left\langle \begin{pmatrix} 4 \\ 226 \end{pmatrix}, \begin{pmatrix} 0 \\ 4 \end{pmatrix} \right\rangle \right) \rtimes \mathbb{Z} \cong \left(\mathbb{Z}^2 / \left\langle \begin{pmatrix} 4 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 4 \end{pmatrix} \right\rangle \right) \rtimes \mathbb{Z} \cong (\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}.$$

- (5) if $g = a^2 b^2 c^2$, we have $d = 2$, $m = 3$, $D = 1$. In this case, $b^4 =_G c^2 =_G 1$ and the quotient group is isomorphic to $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}$ with the action given by $aba^{-1} = b^3$. This is a two-step-nilpotent quotient of the Baumslag-Solitar group $BS(1, 3)$ by introducing the relation $b^4 = 1$.

We see that the quotient group G collapses down to \mathbb{Z} precisely if $\gcd(i, j) = 1$. Namely, $c =_G 1$ in that case, so we have a quotient of \mathbb{Z}^2 by a primitive vector.

Corollary 27. For one-relator quotients of the Heisenberg group, $G = N_{2,2}/\langle\langle g \rangle\rangle$,

$$\Pr(G \cong \mathbb{Z}) = \frac{6}{\pi^2} \approx 60.8\% ; \quad \Pr(G \text{ step 2, rank 2}) = 1 - \frac{6}{\pi^2}.$$

Of course, if $g = c$, we have \mathbb{Z}^2 , but this event occurs with probability zero. If $\gcd(i, j) \neq 1$, then G is two-step (thus non-abelian) and has torsion.

Proof of theorem. First, the $(i, j) = (0, 0)$ case is very straightforward: then $g = c^k$ and the desired expression for G follows.

Below, we assume $(i, j) \neq (0, 0)$, and by Lemma 5, without loss of generality, we will write $g = b^d c^m$.

Consider the normal closure of b , which is $\langle\langle b \rangle\rangle = \langle b, c \rangle$. This intersects trivially with $\langle a \rangle$, and $G = \langle\langle b \rangle\rangle \langle a \rangle$. Thus $G = \langle b, c \rangle \rtimes \langle a \rangle$.

Now in $H(\mathbb{Z})$, we compute $\langle\langle g \rangle\rangle = \langle b^d c^m, c^d \rangle \subset \langle b, c \rangle$. Thus

$$\langle b, c \rangle \cong \mathbb{Z}^2 / \left\langle \begin{pmatrix} d \\ m \end{pmatrix}, \begin{pmatrix} 0 \\ d \end{pmatrix} \right\rangle.$$

We have the semidirect product structure $G \cong \mathbb{Z}^2 / \langle \binom{d}{m}, \binom{0}{d} \rangle \rtimes \mathbb{Z}$, where the action sends $\binom{1}{0} \mapsto \binom{1}{1}$ and fixes $\binom{0}{1}$. Note that c has order d in G , and a simple calculation verifies that b has order d^2/D , where $D = \gcd(d, m)$. If we are willing to lose track of the action and just write the group up to isomorphism, then we can perform both row and column operations on $\begin{bmatrix} d & 0 \\ m & d \end{bmatrix}$ to get $\begin{bmatrix} d^2/D & 0 \\ 0 & D \end{bmatrix}$, which produces the desired expression. \square

In fact, we can say something about quotients of $H(\mathbb{Z})$ with arbitrary numbers of relators. First let us define the K -factor $K(R)$ of a relator set $R = \{g_1, \dots, g_r\}$, where relator g_1 has the Mal'cev coordinates (i_1, j_1, k_1) , and similarly for g_2, \dots, g_r . Let $M = \begin{pmatrix} i_1 & i_2 & \dots & i_r \\ j_1 & j_2 & \dots & j_r \end{pmatrix}$ and suppose its nullity (the dimension of its kernel) is q . Then let W be a kernel matrix of M , i.e., an $r \times q$ matrix with rank q such that $MW = \mathbf{0}$. (Note that if R is a random relator set, then $q = r - 2$, since the rank of M is 2 with probability one.) Let $k = (k_1, \dots, k_r)$ be the vector of c -coordinates of relators, so that $kW \in \mathbb{Z}^q$. Then $K(R) := \gcd(kW)$ is defined to be the gcd of those q integers.

Theorem 28 (Orders of Heisenberg quotients). Consider the group $G = H(\mathbb{Z}) / \langle\langle g_1, \dots, g_r \rangle\rangle$, where relator g_1 has the Mal'cev coordinates (i_1, j_1, k_1) , and similarly for g_2, \dots, g_r . Let $d = \gcd(i_1, j_1, \dots, i_r, j_r)$; let Δ be the co-area of the lattice spanned by the $\binom{i_\alpha}{j_\alpha}$ in \mathbb{Z}^2 ; and let $K = K(R)$ be the K -factor defined above. Then c has order $\gamma = \gcd(d, K)$ in G and $|G| = \Delta \cdot \gamma$.

Proof. Clearly Δ is the order of $\text{ab}(G) = G / \langle c \rangle$. So to compute the order of G , we just need to show that the order of c in G is γ . Consider for which n we can have $c^n \in \langle\langle g_1, \dots, g_r \rangle\rangle$, i.e.,

$$c^n = \prod_{\alpha=1}^N w_\alpha g_\alpha^{\epsilon_\alpha} w_\alpha^{-1}$$

for arbitrary words w_α and integers ϵ_α . First note that all commutators $[w, g_\alpha]$ are of this form, and that by letting $w = a$ or b , these commutators can equal c^{i_α} or c^{j_α} for any α , so n can be an arbitrary multiple of d .

Next, consider the expression in full generality and note that $\mathbf{A}(c^n) = \binom{0}{0}$. Conjugation preserves weights, so $\mathbf{A}(w_\alpha g_\alpha^{\epsilon_\alpha} w_\alpha^{-1}) = \mathbf{A}(g_\alpha^{\epsilon_\alpha}) = \epsilon_\alpha \mathbf{A}(g_\alpha) = \epsilon_\alpha \binom{i_\alpha}{j_\alpha}$. To get the two sides to be equal in abelianization, the ϵ_α must record a linear dependency in the $\binom{i_\alpha}{j_\alpha}$. Finally we compute

$$n = \sum_{\alpha} \epsilon_\alpha (x_\alpha j_\alpha - y_\alpha i_\alpha) + \sum_{\alpha < \beta} \epsilon_\alpha \epsilon_\beta i_\beta j_\alpha - \sum_{\alpha} i_\alpha j_\alpha \frac{\epsilon_\alpha (\epsilon_\alpha - 1)}{2} + \sum_{\alpha} \epsilon_\alpha k_\alpha,$$

where $\binom{x_\alpha}{y_\alpha} = \mathbf{A}(w_\alpha)$. We can observe that each of the first three terms is a multiple of d and the fourth term is an arbitrary integer multiple of K . (To see this, note that the column span of W is exactly the space of linear dependencies in the $\mathbf{A}(g_\alpha)$, so $\sum \epsilon_\alpha k_\alpha$ is a scalar product of the k vector with something in that column span, and is therefore a multiple of K .) Thus n can be any integer combination of d and K , as we needed to prove. \square

We will include experimental data about the distribution of random Heisenberg quotients in Section 7.

5. RANK DROP

First, we establish that adding a single relator to a (sufficiently complicated) free nilpotent group does not drop the nilpotency class; the rank drops by one if the relator is primitive in abelianization and it stays the same otherwise. Furthermore, a single relator never drops the step unless the starting rank was two. This is a nilpotent version of Magnus's famous *Freiheitssatz* (freeness theorem) for free groups [10, Thm 4.10].

Theorem 29 (Nilpotent *Freiheitssatz*). For any $g \in N_{s,m}$ with $s \geq 2, m \geq 3$, there is an injective homomorphism

$$N_{s,m-1} \hookrightarrow N_{s,m} / \langle\langle g \rangle\rangle.$$

This is an isomorphism if and only if $\gcd(A_1(g), \dots, A_m(g)) = 1$.

If $m = 2$ the result holds with $\mathbb{Z} \hookrightarrow N_{s,2}/\langle\langle g \rangle\rangle$.

Proof. Romanovskii's 1971 theorem [14, Thm 1] does most of this. In our language, the theorem says that if $A_m(g) \neq 0$, then $\langle a_1, \dots, a_{m-1} \rangle$ is a copy of $N_{s,m-1}$. This establishes the needed injection except in the case $g \in [N_{s,m}, N_{s,m}]$, where $\mathbf{A}(g)$ is the zero vector. In the $m = 2$ case, any such $N_{s,2}/\langle\langle g \rangle\rangle$ has abelianization \mathbb{Z}^2 , so the statement holds. For $m > 2$, one can apply an automorphism so that g is spelled with only commutators involving a_m . Even killing all such commutators does not drop the nilpotency class because $m > 2$ ensures that there are some Mal'cev generators spelled without a_m in each level. Thus in this case $\langle a_1, \dots, a_{m-1} \rangle \cong N_{s,m-1}$ still embeds.

It is easy to see that if g is non-primitive in abelianization, then the rank of $\text{ab}(N_{s,m}/\langle\langle g \rangle\rangle)$ is m , and so the quotient nilpotent group has rank m as well. However, the image of Romanovskii's map has rank $m - 1$, so it is not a surjection.

On the other hand, suppose $\text{ab}(g)$ is a primitive vector. Then the rank of the abelianized quotient is $m - 1$, and by Magnus's theorem (Theorem 3) the rank of the nilpotent quotient is the same. The group $G = N_{s,m}/\langle\langle g \rangle\rangle$ is therefore realizable as a quotient of that copy of $N_{s,m-1}$. Since the lower central series of $N_{s,m-1}$ has all free abelian quotients, any proper quotient would have smaller Hirsch length, and this contradicts Romanovskii's injection. Thus relative primality implies that the injection is an isomorphism. \square

Now we can use rank drop to analyze the probability of an abelian quotient for a free nilpotent group in the underbalanced, nearly balanced, and balanced cases (i.e., cases with the number of relators at most the rank).

Lemma 30 (Abelian implies rank drop for up to m relators). Let $G = N_{s,m}/\langle\langle R \rangle\rangle$, where $R = \{g_1, \dots, g_r\}$ is a set of $r \leq m$ random relators. Suppose $s \geq 2$ and $m \geq 2$. Then

$$\Pr(G \text{ abelian} \mid \text{rank}(G) = m) = 0.$$

Proof. Suppose that $\text{rank}(G) = m$ and G is abelian. We use the form of the classification of abelian groups (Remark 7) in which $G \cong \oplus_{i=1}^m \mathbb{Z}/d_i\mathbb{Z}$, where $d_m \mid \dots \mid d_1$ so that $d_1 = \dots = d_q = 0$ for $q = \dim(G)$, and we write $\langle\langle \text{ab}(R) \rangle\rangle = \langle d_1 e_1, \dots, d_m e_m \rangle$ for a basis $\{e_i\}$ of \mathbb{Z}^m . Since $\text{rank}(G) = m$, we can assume no $d_i = 1$. We can lift the basis $\{e_i\}$ of \mathbb{Z}^m to a generating set $\{a_i\}$ of $N_{s,m}$ by Magnus (Theorem 3). Note that the exponent of each generator in each relator is a multiple of d_m .

Next we show that we cannot kill a commutator in G without dropping rank. Let $b_1 = [a_1, a_m]$. We claim that $b_1 \notin \langle\langle g_1, \dots, g_r \rangle\rangle$. To do so, we compute an arbitrary element

$$\prod_{\alpha}^n w_{\alpha} g_{\alpha}^{\epsilon_{\alpha}} w_{\alpha}^{-1} \in \langle\langle g_1, \dots, g_r \rangle\rangle.$$

Conjugation preserves weights, so $\mathbf{A}(w_{\alpha} g_{i_{\alpha}}^{\epsilon_{\alpha}} w_{\alpha}^{-1}) = \mathbf{A}(g_{i_{\alpha}}^{\epsilon_{\alpha}}) = \epsilon_{\alpha} \mathbf{A}(g_{i_{\alpha}})$. If the product is equal to b_1 , then its a -weights are all zero. Now consider the b -weights. For the product, the b -weights are the combination of the b -weights of the g_{α} , modified by amounts created by commutation. However, since all the a -exponents of all the g_{α} are multiples of d_m , we get

$$\sum \epsilon_i \mathbf{A}(g_i) = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \sum \epsilon_i \mathbf{B}(g_i) \equiv \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \pmod{d_m},$$

where each ϵ_i is the sum of the ϵ_{α} corresponding to g_i . The second expression ensures that the ϵ_i are not all zero, so the first equality is a linear dependence in the $\mathbf{A}(g_i)$, which has probability zero since $r \leq m$. \square

Theorem 31. (Underbalanced quotients are not abelian) Let $G = N_{s,m}/\langle\langle R \rangle\rangle$, where $R = \{g_1, \dots, g_r\}$ is a set of $r \leq m - 2$ random relators g_i . Then

$$\Pr(G \text{ abelian}) = 0.$$

Proof. Suppose that G is abelian, and consider elements of G as vectors in \mathbb{Z}^m via the abelianization map on $N_{s,m}$; in this way we get vectors $v_1 = \mathbf{A}(g_1), \dots, v_r = \mathbf{A}(g_r)$. From the previous result we may assume $\text{rank}(G) < m$. By Lemma 8, we can find a primitive vector w as a linear combination of the v_i . Then we apply the linear algebra lemma (Lemma 10) to extend w appropriately so that $\text{span}(v_1, \dots, v_r) = \text{span}(w, w_2, \dots, w_r)$. We can find a series of elementary row operations (switching, multiplication by -1 , or addition) to get (w, w_2, \dots, w_r) from (v_1, \dots, v_r) , and we lift these operations to elementary Nielsen transformations (switching, inverse, or multiplication, respectively) in $N_{s,m}$ to get (g', g'_2, \dots, g'_r) from (g_1, \dots, g_r) . Note that Nielsen transformations on a set of group elements preserve the subgroup they generate, so also preserve normal closure. This lets us define $R' = \{g', g'_2, \dots, g'_r\}$ with $\langle\langle R' \rangle\rangle = \langle\langle R \rangle\rangle$. Since g' has a weight vector w whose coordinates are relatively prime, the Freiheitssatz (Theorem 29) ensures that $N_{s,m}/\langle\langle g' \rangle\rangle \cong N_{s,m-1}$. Thus we have $G = N_{s,m-1}/\langle\langle g'_2, \dots, g'_r \rangle\rangle$.

If $r \leq m-2$, then iterating this argument $r-1$ times gives $G \cong N_{s,m-r+1}/\langle\langle g_r \rangle\rangle$ for some new g_r , and $m-r+1 \geq 3$. Then we can apply Theorem 29 to conclude that this quotient is not abelian, because its nilpotency class is $s > 1$. \square

Proposition 32 (Cyclic quotients). If $|R| = m-1$ or $|R| = m$, then abelian implies cyclic:

$$\Pr(G \text{ cyclic} \mid G \text{ abelian}) = 1.$$

Proof. Running the proof as above, we iterate the reduction $m-2$ times to obtain $G \cong N_{s,2}/\langle\langle g \rangle\rangle$ or $N_{s,2}/\langle\langle g, g' \rangle\rangle$.

If g (or any element of $\langle\langle g, g' \rangle\rangle$) is primitive, then G is isomorphic to \mathbb{Z} or a quotient of \mathbb{Z} , i.e., G is cyclic.

Otherwise, note that $N := N_{s,2}$ has the Heisenberg group as a quotient ($H(\mathbb{Z}) = N_1/N_3$). If G is abelian, then the corresponding quotient of $H(\mathbb{Z})$ is abelian. In the non-primitive case, this can only occur if $c \in \langle\langle g, g' \rangle\rangle$, which (as in the proof of Lemma 30) implies $\mathbf{A}(g) = (0,0)$ (or a linear dependency between $\mathbf{A}(g)$ and $\mathbf{A}(g')$). But by Corollary 14, the changes of basis do not affect the probability of linear dependency, so this has probability zero. \square

Corollary 33. For nearly-balanced and balanced models, the probability that a random nilpotent group is abelian equals the probability that it is cyclic.

We reprise the table from §3, recalling that values are truncated at four digits.

$\Pr(\text{abelian})$	$m = 2$	$m = 3$	$m = 4$	$m = 10$	$m = 100$	$m = 1000$	$m \rightarrow \infty$
$ R = m-1$.6079	.5057	.4672	.4361	.4357	.4357	.4357
$ R = m$.9239	.8842	.8651	.8469	.8469	.8469	.8469

Corollary 34 (Abelian one-relator). For any step $s \geq 2$,

$$\Pr(N_{s,m}/\langle\langle g \rangle\rangle \text{ is abelian}) = \begin{cases} 6/\pi^2, & m = 2 \\ 0, & m \geq 3. \end{cases}$$

Note that these last two statements agree for $m = 2$, $|R| = m-1 = 1$.

6. TRIVIALIZING AND PERFECTING RANDOM GROUPS

In this final section, we first observe the low threshold for collapse of a random nilpotent group, using the abelianization. Then we will prove a statement lifting facts about random nilpotent group to facts about the LCS of classical random groups, deducing that *random groups are perfect* with the same threshold again.

Recall that $T_{j,m} = \{[a_{i_1}, \dots, a_{i_j}] : 1 \leq i_1, \dots, i_j \leq m\}$ contains the basic nested commutators with j arguments. In this section we fix m and write F for the free group, so we can write F_i for the groups in its lower central series. Similarly we write N for $N_{s,m}$ (when s is understood), and T_j for $T_{j,m}$. Note that $\langle\langle T_j \rangle\rangle = F_j$, so $N = F/F_{s+1}$.

For a random relator set $R \subset F$, we write $\Gamma = F/\langle\langle R \rangle\rangle$, $G = N/\langle\langle R \rangle\rangle$, and $H = \mathbb{Z}^m/\langle R \rangle = \text{ab}(\Gamma) = \text{ab}(G)$, using the abuse of notation from Lemma 11 and treating R as a set of strings from F to be identified with its image in N or \mathbb{Z}^m . In all cases, R is chosen uniformly from words of length ℓ or $\ell - 1$ in F .

First we need a result describing the divisibility properties of the determinants of matrices whose columns record the coordinates of random relators.

Lemma 35 (Common divisors of random determinants). Fixing m and any $k > 10m$, let $d_\ell^{(k)} = \gcd(\Delta_{\ell,1}, \dots, \Delta_{\ell,k})$ be the greatest common divisor of the determinants of k random $m \times m$ matrices all of whose columns are independently sampled from \hat{A}_ℓ . Then, as $\ell \rightarrow \infty$,

$$\Pr(d_\ell^{(k)} = 1) \longrightarrow \prod_{\text{primes } p} 1 - \left[1 - \left(1 - \frac{1}{p} \right) \left(1 - \frac{1}{p^2} \right) \cdots \left(1 - \frac{1}{p^m} \right) \right]^k.$$

To prove this carefully requires dividing the primes into size ranges and verifying that only the small primes ($p \leq \log \log \ell$) contribute. See the Appendix [3] for details.

The following theorem tells us that in sharp contrast to Gromov random groups, where the number of relators required to trivialize the group is exponential in ℓ , even the slowest-growing unbounded functions, like $\log \log \log \ell$ or an inverse Ackermann function, suffice to collapse random abelian groups and random nilpotent groups.

Theorem 36 (Collapsing abelian quotients). For random abelian groups $H = \mathbb{Z}^m/\langle R \rangle$ with $|R|$ random relators, if $|R| \rightarrow \infty$ as a function of ℓ , then $H = \{0\}$ with probability one (a.a.s.). If $|R|$ is bounded as a function of ℓ , then there is a positive probability of a nontrivial quotient, both for each ℓ and asymptotically.

Proof. For a relator g of length ℓ , its image in \mathbb{Z}^m is the random vector $\mathbf{A}(g)$, which converges in distribution to a multivariate normal, as described in §2. Furthermore, the image of this vector in projection to $\mathbb{Z}/p\mathbb{Z}$ has entries that are asymptotically independently and uniformly distributed. We will consider adding vectors to this collection R until they span \mathbb{Z}^m , which suffices to get $H = \{0\}$.

Choose m vectors v_1, \dots, v_m in \mathbb{Z}^m at random. These vectors are a.a.s. \mathbb{R} -linearly independent, because their distribution is normal and linear dependence is a codimension-one condition. Therefore they span a sublattice $L_1 \subset \mathbb{Z}^m$. The covolume of L_1 (i.e., the volume of the fundamental domain) is $\Delta_{\ell,1} = \det(v_1, \dots, v_m)$. As we add more vectors, we refine the lattice. Note that $\Delta_{\ell,1} = 1$ if and only if $L_1 = \mathbb{Z}^m$. Similarly define L_j to be spanned by $v_{(j-1)m+1}, \dots, v_{jm}$ for $j = 2, 3, \dots$, and define $\Delta_{\ell,j}$ to be the corresponding covolumes.

Note that for two lattices L, L' , the covolume of the lattice $L \cup L'$ is always a common divisor of the respective covolumes Δ, Δ' . Therefore, the lattice $L_1 \cup \dots \cup L_k$ has covolume $\leq \gcd(\Delta_{\ell,1}, \dots, \Delta_{\ell,k})$. From Lemma 35, this gcd approaches

$$\prod_{\text{primes } p} 1 - \left[1 - \left(1 - \frac{1}{p} \right) \left(1 - \frac{1}{p^2} \right) \cdots \left(1 - \frac{1}{p^m} \right) \right]^k,$$

as $\ell \rightarrow \infty$, and this in turn goes to 1 as $k \rightarrow \infty$. (To see this, note that first applying a logarithm, then exchanging the sum and the limit, gives an absolutely convergent sequence.)

On the other hand, it is immediate that for any finite $|R|$ there is a small but nonzero chance that all entries are even, say, which would produce a nontrivial quotient group. \square

Of course this also follows immediately from the statement in Lemma 23, because

$$\Pr(\text{span}\{v_1, \dots, v_r\} = \mathbb{Z}^m) = \frac{1}{\zeta(r-m+1) \cdots \zeta(r)} \longrightarrow 1$$

for any fixed m as $r \rightarrow \infty$.

We immediately get corresponding statements for random nilpotent groups and standard random groups. Recall that a group Γ is called *perfect* if $\Gamma = [\Gamma, \Gamma]$; equivalently, if $\text{ab}(\Gamma) = \Gamma/[\Gamma, \Gamma] = \{0\}$.

Corollary 37 (Threshold for collapsing random nilpotent groups). A random nilpotent group $G = N_{s,m}/\langle\langle R \rangle\rangle$ is a.a.s. trivial precisely in those models for which $|R| \rightarrow \infty$ as a function of ℓ .

Corollary 38 (Random groups are perfect). Random groups $\Gamma = F_m/\langle\langle R \rangle\rangle$ are a.a.s. perfect precisely in those models for which $|R| \rightarrow \infty$ as a function of ℓ .

Proof. $\mathbb{Z}^m/\langle R \rangle = \{0\} \iff \text{ab}(\Gamma) = \{0\} \iff \text{ab}(G) = \{0\} \iff G = \{1\}$, with the last equivalence from Theorem 3. \square

We have established that the collapse to triviality of a random nilpotent group G corresponds to the immediate stabilization of the lower central series of the corresponding standard random group: $\Gamma_1 = \Gamma_2 = \dots$. In fact, we can be somewhat more detailed about the relationship between G and the LCS of Γ .

Theorem 39 (Lifting to random groups). For $\Gamma = F_m/\langle\langle R \rangle\rangle$ and $G = N_{s,m}/\langle\langle R \rangle\rangle$, they are related by the isomorphism $\Gamma/\Gamma_{s+1} \cong G$. Furthermore, the first s of the successive LCS quotients of Γ are the same as those in the LCS of G , i.e.,

$$\Gamma_i/\Gamma_{i+1} \cong G_i/G_{i+1} \quad \text{for } 1 \leq i \leq s.$$

Proof. Since homomorphisms respect LCS depth (Lemma 19), the quotient map $\phi : F \rightarrow \Gamma$ gives $\phi(F_j) = \Gamma_j$ for all j . We have

$$\Gamma/\Gamma_{s+1} \cong F/\langle\langle R, F_{s+1} \rangle\rangle \cong N/\langle\langle R \rangle\rangle = G$$

by Lemma 11 (string arithmetic).

From the quotient map $\psi : \Gamma \rightarrow G$, we get $\Gamma_i/\Gamma_{s+1} = \psi(\Gamma_i) = G_i$. Thus

$$G_i/G_{i+1} \cong \Gamma_i/\Gamma_{s+1}/\Gamma_{i+1}/\Gamma_{s+1} \cong \Gamma_i/\Gamma_{i+1}. \quad \square$$

Corollary 40 (Step drop implies LCS stabilization). For $G = N_{s,m}/\langle\langle R \rangle\rangle$, if $\text{step}(G) = k < s = \text{step}(N_{s,m})$, then the LCS of the random group Γ stabilizes: $\Gamma_{k+1} = \Gamma_{k+2} = \dots$.

Proof. This follows directly from the previous result, since $\text{step}(G) = k$ implies that $G_{k+1} = G_{k+2} = 1$, which means $G_{k+1}/G_{k+2} = 1$. Since $k+1 \leq s$, we conclude that $\Gamma_{k+1}/\Gamma_{k+2} = 1$. Thus $\Gamma_{k+2} = \Gamma_{k+1}$, and it follows by the definition of LCS that these also equal Γ_i for all $i \geq k+1$. \square

Thus, in particular, when a random nilpotent group (with $m \geq 2$) is abelian but not trivial, the corresponding standard random group has its lower central series stabilize after one proper step:

$$\dots \Gamma_4 = \Gamma_3 = \Gamma_2 \triangleleft \Gamma_1 = \Gamma$$

For instance, with balanced quotients of F_2 this happens about 92% of the time.

In future work, we hope to further study the distribution of steps for random nilpotent groups.

7. EXPERIMENTS

7.1. Multi-relator Heisenberg quotients. The following table records the outcomes of 10,000 trials (1000 trials for each of the ten rows) with relators of length 999 and 1000, for $G = H(\mathbb{Z})/\langle\langle R \rangle\rangle$. Note that $|R| = 2$ is the balanced case.

	$ G = 1$ (trivial)	G cyclic nontrivial (rk 1)		G abelian noncyclic (rk 2 step 1)		G nonabelian (rk 2 step 2)		largest finite order
		infinite	finite	infinite	finite	infinite	finite	—
$ R = 1$	0	604	0	0	0	396	0	—
2	1	1	917	0	0	0	81	11178
3	514	0	467	0	9	0	10	717
4	766	0	228	0	2	0	4	104
5	884	0	116	0	0	0	0	7
6	945	0	55	0	0	0	0	4
7	979	0	21	0	0	0	0	3
8	981	0	19	0	0	0	0	3
9	995	0	5	0	0	0	0	2
10	997	0	3	0	0	0	0	2

Note that the triviality column comports closely with the probability of collapse described in §3:

$$\Pr(\text{span}\{v_1, \dots, v_r\} = \mathbb{Z}^2) = \frac{1}{\zeta(r-1) \cdot \zeta(r)},$$

which predicts 0, 0, 506, 769, 891, 948, 975, 988, 994, and 997 trivial quotients.

7.2. Finite nonabelian quotients of balanced presentations. Because underbalanced ($|R| \leq m - 2$) and nearly-balanced ($|R| = m - 1$) presentations necessarily produce infinite groups, while the overbalanced case ($|R| \geq m + 1$) often collapses the group, balanced presentations are a good source for finite nonabelian quotients, as one sees in the table above. Consider balanced quotients of $H(\mathbb{Z})$ for which the random relators have Mal'cev coordinates (i_1, j_1, k_1) and (i_2, j_2, k_2) . Letting $\Delta = |i_1 j_2 - i_2 j_1|$, the group is finite if and only if $\Delta > 0$, in which case the order of the abelianization is Δ . Letting $d = \gcd(i_1, j_1, i_2, j_2)$, we recall that $d = 1$ implies a cyclic quotient, so the finite nonabelian case requires $\Delta > 0$ and $d > 1$. Having $\Delta > 0$ implies that there are no nontrivial linear dependencies between $\begin{pmatrix} i_1 \\ j_1 \end{pmatrix}$ and $\begin{pmatrix} i_2 \\ j_2 \end{pmatrix}$, so $K(R) = 0$ (as in Theorem 28), making the order of c in the quotient group equal to d ; since $|c| = d$, the quotient is nonabelian iff $d > 1$. Finally $|G| = \Delta \cdot d$, and we further note that $d^2 \mid \Delta$, so d^3 divides the order of the group. This means that the smallest possible orders of nonabelian quotients are 8, 16, 24, 27, 32, 40, 48, 54, ...

With small-order groups, one can easily classify by isomorphism type, asking for instance how many of the order-eight nonabelian groups are isomorphic to the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ and how many to the dihedral group D_4 . However, since the expected magnitude of each of the entries in $\begin{pmatrix} i_1 \\ j_1 \end{pmatrix}$ and $\begin{pmatrix} i_2 \\ j_2 \end{pmatrix}$ is $\sqrt{\ell}$, the value of Δ and hence the expected size of these quotient groups is growing fast with ℓ . Therefore to illustrate the distribution of random nilpotent groups that are small-order nonabelian, we consider $n = 10,000$ trials with $\ell = 9$ or 10. In this sample, 562 of the quotients were finite nonabelian.

order	8	16	24	27	32	40	48	54	56	64	72	80	81	88	96	125	216
frequency	130	138	65	41	45	32	35	24	9	18	9	3	6	1	2	2	2

Of the 130 groups in this sample of order eight, 33 were isomorphic to Q , and the other 97 to D_4 .

7.3. One-relator Heisenberg quotients. Finally, we use Lemma 5 and Theorem 25 to study the diversity of random infinite groups appearing in the one-relator case. Given a random relator whose Mal'cev coordinates are (i, j, k) , we first change variables as in the Lemma to obtain coordinates $(0, d, m)$, where $d = \gcd(i, j)$ and $m = \frac{ij}{2d}(d-1) + k$. In this presentation, as noted in the proof of the Theorem, $\text{ord}(c) = d$ and $\text{ord}(b) = d^2/D$, while a has infinite order. Thus every word involving a has infinite order; on the other hand, b and c commute and so any word in those letters alone has order at most d^2/D (note that this is divisible by d because $D = \gcd(d, m)$). Extracting information that is independent of presentation, we conclude that the order of the center is d and the largest order of a torsion element is d^2/D .

We ran $n = 20,000$ trials with $\ell = 999$ or 1000 and plotted the frequency of each $(d^2/D, d)$ pair (Figure 2). Besides the groups that are pictured, there were also four occurrences of $(i, j) = (0, 0)$ in the sample, with k values $55, 187, 230, 580$, that are not pictured. Because groups with distinct $(d^2/D, d)$ pairs must be non-isomorphic, our sample contains at least 202 distinct groups (up to isomorphism).

Recall from Remark 26 that groups with $D = 1$ are called Baumslag-Solitar type because they are isomorphic quotients of some $BS(1, q)$. But $D = \gcd(d, m)$, and from the expression $m = \frac{ij}{2d}(d-1) + k$ we can note that $2d \mid ij$ if either i or j is even, in which case $\gcd(d, m) = \gcd(i, j, k)$. (If both are odd, the situation splits into sub-cases depending on the 2-adic valuations.) This suggests heuristically that non-cyclic groups of Baumslag-Solitar type should occur with probability $\frac{1}{\zeta(3)} - \frac{1}{\zeta(2)} = .22398\dots$. The precise frequency of groups of this type in the sample was 4404, or 22.02%.

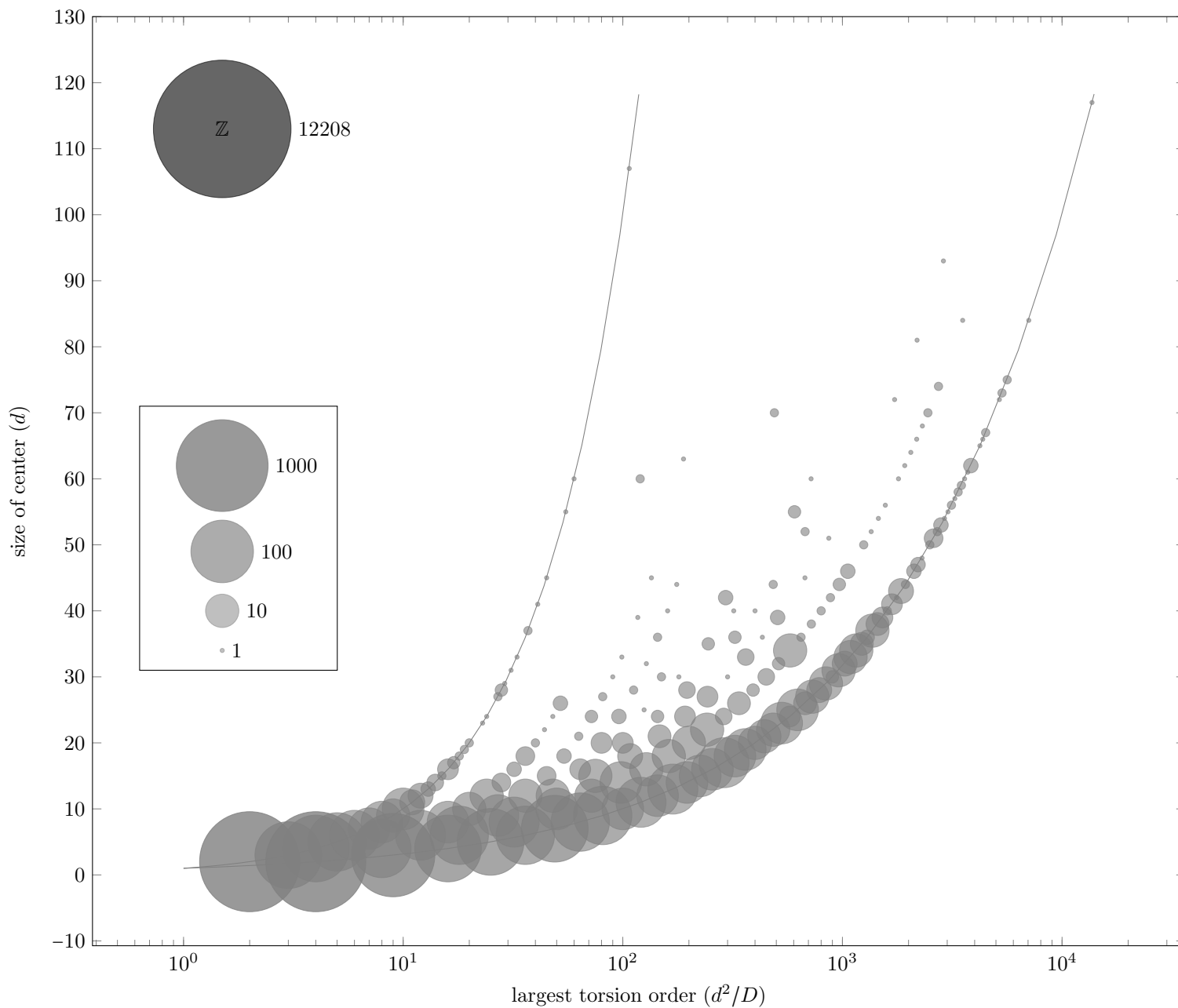


FIGURE 2. A semilog plot of $(d^2/D, d)$ in 20,000 random 1-relator quotients of the Heisenberg group with relator length 999 or 1000, showing at least 202 mutually non-isomorphic groups. Various sized disks represent the number of occurrences of each $(d^2/D, d)$ value. Since $D|d$, all possibilities lie between the curves (d, d) and (d^2, d) . Of these random groups, 61% are isomorphic to \mathbb{Z} and an additional 22% are of Baumslag-Solitar type ($D = 1 \Rightarrow G \cong BS(1, q)/\langle\langle g \rangle\rangle$ as in Remark 26), and thus lie along the lower curve (d^2, d) .

Funding. This work was initiated in the Random Groups Research Cluster held at Tufts University in Summer 2014, supported by the National Science Foundation [DMS-CAREER-1255442].

Acknowledgments. The co-authors had many stimulating and useful conversations in the course of the work, including with Phil Matchett Wood, Nathan Dunfield, Dylan Thurston, Ilya Kapovich, Anshel Schaffer-Cohen, Rick Kenyon, and Larry Guth. Special thanks to Keith Conrad and to Hannah Alpert for several insightful observations, and to two anonymous referees for close reading and very helpful suggestions. Finally, Melanie Matchett Wood pointed out several issues in the preprint that merited more detail and care, which led to the creation of an appendix. We are extremely grateful for the feedback.

REFERENCES

- [1] E. Breuillard, *Random walks on Lie groups*. <http://www.math.u-psud.fr/~breuilla/part0gb.pdf>
- [2] Drutu and Kapovich, *Lectures on geometric group theory*. Preprint.
- [3] M. Duchin, M. Ho, A. Sánchez, *Appendix to Random Nilpotent Groups I*. <https://arxiv.org/abs/1506.01426>
- [4] M. Duchin, K. Jankiewicz, S. Kilmer, S. Lelièvre, J. Mackay, and A. Sánchez, *A sharper threshold for random groups at density one-half*. Groups, Geometry, and Dynamics, Vol 10, Issue 3, 2016, 985–1005.
- [5] N. Dunfield and W. Thurston, *Finite covers of random 3-manifolds*. Invent. Math. 166 (2006), no. 3, 457–521.
- [6] R. Fitzner and R. van der Hofstad, *Non-backtracking random walk*. Journal of Statistical Physics 150(2): 264–284, (2013).
- [7] Marshall Hall, Jr., *The theory of groups*. Second edition. American Mathematical Society, 1976.
- [8] Hardy and Wright, *An introduction to the theory of numbers*. Sixth edition. Oxford University Press, 2008.
- [9] R. Kravchenko, M. Mazur, and B. Petrenko, *On the smallest number of generators and the probability of generating an algebra*. Algebra Number Theory 6 (2012), no. 2, 243–291.
- [10] Wilhelm Magnus, Abraham Karrass, Donald Solitar, *Combinatorial group theory. Presentations of groups in terms of generators and relations*. Second edition. Dover, 1975.
- [11] J. Nielsen, *Die Isomorphismen der allgemeinen, unendlichen Gruppe mit zwei Erzeugenden*. (German) Math. Ann. 78 (1917), no. 1, 385–397.
- [12] Yann Ollivier, *A January 2005 Invitation to Random Groups*, Ensaios Matemáticos [Mathematical Surveys], vol. 10, Sociedade Brasileira de Matemática, Rio de Janeiro, 2005, 31, 85–86.
- [13] Derek J.S. Robinson, *A course in the theory of groups*, 2nd ed., Springer-Verlag, 1996.
- [14] N.S. Romanovskii, *A freedom theorem for groups with one defining relation in the varieties of solvable and nilpotent groups on given lengths*. (English translation.) Math. USSR-Sb. 18 (1972), 93–99.
- [15] L. Saloff-Coste, *Random walks on finite groups*. Probability on discrete structures, 263–346, Encyclopaedia Math. Sci., 110, Springer, Berlin, 2004.
- [16] Charles C. Sims, *Computation with finitely presented groups*. Encyclopedia of Mathematics and its Applications, 48. Cambridge University Press, Cambridge, 1994.
- [17] Yinghui Wang and Richard P. Stanley, *The Smith normal form distribution of a random integer matrix*. <https://arxiv.org/abs/1506.00160>
- [18] Melanie Matchett Wood, *Random integral matrices and the Cohen Lenstra Heuristics*. <https://arxiv.org/abs/1504.04391>

APPENDIX A. EXPANDED INFORMATION ON ARITHMETIC PROPERTIES OF RANDOM WALKS

MOON DUCHIN, MENG-CHE HO, AND ANDREW SÁNCHEZ

This appendix fills in details for some claims given above about arithmetic properties of random walks. We will focus here on the simple random walk (SRW) on \mathbb{Z}^m , where the arguments will be spelled out in full, but also give indications of how to extend these arguments to non-backtracking simple random walk (NBSRW). We will use the notation \hat{A}_ℓ for the \mathbb{Z}^m -valued random walk, as above, and discuss the SRW and the NBSRW case separately in each argument below.

If E_ℓ is an event that depends on a parameter ℓ , we use the symbol $\Pr(E_\ell)$ for the probability for fixed ℓ and write $\overline{\Pr}(E_\ell) := \lim_{\ell \rightarrow \infty} \Pr(E_\ell)$ for the asymptotic probability. If E is an event with respect to a matrix-valued random variable, we use the notation $\Pr'(E)$ to denote the conditional probability of E given that no matrix entries are zero.

We will analyze primes by their size relative to ℓ , so we fix a small ϵ (say $0 < \epsilon < \frac{1}{10}$) and define size ranges:

$$\mathcal{P}_1 := \{p \leq \log \log \ell\} \quad \mathcal{P}_2 := \{\log \log \ell \leq p \leq \ell^{\frac{1}{2}-\epsilon}\} \quad \mathcal{P}_3 := \{\ell^{\frac{1}{2}-\epsilon} \leq p \leq \ell^{m+1}\} \quad \mathcal{P}_4 := \{p \geq \ell^{m+1}\}.$$

Recall that Lemma 15 provides that $\exists c_1, c_2 > 0$ s.t. $\forall n < \ell^{\frac{1}{2}-\epsilon}, \forall 1 \leq s \leq m, \forall k_1, \dots, k_s$,

$$\Pr(\hat{A}_{\ell, i_1} \equiv k_1, \dots, \hat{A}_{\ell, i_s} \equiv k_s \pmod n) < \frac{1}{n^s} + c_1 e^{-c_2 \ell^{2\epsilon}}.$$

Here we will carefully establish the following two results from above.

Corollary 17 (Probability of primitivity). For a random freely reduced word in F_m , the probability that it is primitive in abelianization tends to $1/\zeta(m)$, where ζ is the Riemann zeta function. In particular, for $m = 2$, the probability is $6/\pi^2$.

Lemma 35 (Common divisors of random determinants). Fixing m and any $k > 10m$, let $d_\ell^{(k)} = \gcd(\Delta_{\ell, 1}, \dots, \Delta_{\ell, k})$ be the greatest common divisor of the determinants of k random $m \times m$ matrices all of whose columns are independently sampled from \hat{A}_ℓ . Then, as $\ell \rightarrow \infty$,

$$\Pr(d_\ell^{(k)} = 1) \longrightarrow \prod_{\text{primes } p} 1 - \left[1 - \left(1 - \frac{1}{p} \right) \left(1 - \frac{1}{p^2} \right) \dots \left(1 - \frac{1}{p^m} \right) \right]^k.$$

Probability of primitivity. For SRW, $\hat{A}_{\ell, i}$ proceeds like a lazy simple random walk on \mathbb{Z} : at each step, it advances left or right with probability $1/2m$, and otherwise it stands still. A similar statement is true for NBSRW, but the probabilities depend on the previous step. As mentioned above, classical central limit theorems tell us that $\hat{A}_{\ell, i}$ is asymptotically normally distributed, and this is true for the NBSRW case as well [6]. In this appendix we will sometimes use information about the rate of convergence of $\hat{A}_{\ell, i}$ to the Gaussian distribution. For SRW, we have local central limit theorems (LCLT) which give upper bounds on the difference between the probability that $\hat{A}_{\ell, i} = x$ and the estimate derived from the Gaussian, in terms of x and ℓ (see for instance Lawler-Limic, *Random Walk, A Modern Introduction*, Chapter 2). For NBSRW, this is a folklore result that has not yet been written down, as far as we know.

Lemma A.1 (Divisibility of coordinate projections). For every $m, n \geq 2$, $1 \leq s \leq m$, and $\ell \gg 1$, there is a conditional probability bound given by

$$\Pr'(\hat{A}_{\ell, 1} \equiv \dots \equiv \hat{A}_{\ell, s} \equiv 0 \pmod n) < 1/n^s.$$

In particular, $\Pr(\hat{A}_{\ell, i} \equiv 0 \pmod n \mid \hat{A}_{\ell, i} \neq 0) < 1/n$ for any fixed i .

Proof. We give the detailed argument for $s = 1$. Let $p_\ell(x) = \Pr(\hat{A}_{\ell, i} = x)$. This result will follow from monotonicity of the distribution of $\hat{A}_{\ell, i}$, i.e., $p_\ell(x) > p_\ell(x+1)$ for $x \geq 0$. We proceed by induction on

ℓ . For $\ell = 1$, we have $p_1(0) = \frac{2m-1}{m}$ and $p_1(1) = \frac{1}{4m}$, which establishes the base case. For $\ell > 1$, we have

$$p_\ell(x) = \frac{1}{2m}p_{\ell-1}(x-1) + \frac{m-1}{m}p_{\ell-1}(x) + \frac{1}{2m}p_{\ell-1}(x+1);$$

$$p_\ell(x+1) = \frac{1}{2m}p_{\ell-1}(x) + \frac{m-1}{m}p_{\ell-1}(x+1) + \frac{1}{2m}p_{\ell-1}(x+2).$$

Now we know that $\frac{m-1}{m} > \frac{1}{2m}$ (since $m \geq 2$), and this means

$$\frac{m-1}{m}p_{\ell-1}(x) + \frac{1}{2m}p_{\ell-1}(x+1) > \frac{1}{2m}p_{\ell-1}(x) + \frac{m-1}{m}p_{\ell-1}(x+1),$$

since the LHS has a larger coefficient on the larger term. This compares two of the terms of $p_\ell(x)$ with two of the terms of $p_\ell(x+1)$, so it only remains to compare the remaining terms. Since $x \geq 0$, we have $|x-1| \leq x+1$. Thus, by repeatedly applying the inductive hypothesis, we have $p_{\ell-1}(x-1) > p_{\ell-1}(x+2)$, which completes the proof for all ℓ . In particular, we have shown: if the positive integers $\mathbb{Z}_{>0}$ are partitioned into intervals $[kn+1, kn+n]$, then the farthest point in each interval from 0 (the value divisible by n) has the lowest probability.

For NBSRW, we would need to inspect the LCLT bounds to establish monotonicity rigorously, though it is intuitively clear for $\ell \gg 1$.

The argument for general s runs along exactly the same lines: $\mathbb{Z}_{>0}^m$ is cut up into $n \times \dots \times n$ boxes which are obtained as products of the intervals described above, then in each box, the point farthest from the origin (which satisfies the congruence condition in the statement of the lemma) has the lowest probability in the random walk. \square

Lemma A.2 (Values of coordinate projections). There is a constant c such that for any $\alpha \in \mathbb{Z}$ and any i and $\epsilon > 0$,

$$\Pr(\hat{A}_{\ell,i} = \alpha) < \frac{c}{\sqrt{\ell}} \text{ for } \ell \gg 1.$$

Proof. Bounding $\Pr(\hat{A}_{\ell,i} = \alpha)$ by a multiple of $\ell^{-1/2}$ follows from the standard local central limit theorem for SRW and could be extended to NBSRW from its LCLT. \square

With this, we can establish the probability that a random relator is primitive in abelianization.

Lemma A.3 (Corollary 17). Let δ_ℓ be the greatest common divisor of the entries of $\hat{A}_{\ell,i}$. Then

$$\overline{\Pr}(\delta_\ell > 1) = 1 - \frac{1}{\zeta(m)}.$$

Proof. Recall that for an event expressed in terms of a matrix-valued random variable, $\Pr'(E)$ denotes the conditional probability of E given that the entries of the matrix are nonzero (and this definition makes sense for vectors in particular). Since

$$\Pr(\delta_\ell > 1) \leq \Pr'(\text{some prime divides } \delta_\ell) + \Pr(\text{some entry of } \hat{A}_{\ell,i} \text{ is zero}),$$

we have

$$\begin{aligned} \Pr(\text{some } p \in \mathcal{P}_1 \text{ divides } \delta_\ell) &\leq \Pr(\delta_\ell > 1) \leq \Pr'(\text{some } p \in \mathcal{P}_1 \text{ divides } \delta_\ell) + \Pr'(\text{some } p \in \mathcal{P}_1^c \text{ divides } \delta_\ell) \\ &\quad + \Pr(\text{some entry is zero}). \end{aligned}$$

Recall the (well-known) fact that the product of all primes up to some N is asymptotically e^N ; this implies that $\prod_{p \in \mathcal{P}_1} p < \ell^{\frac{1}{2}-\epsilon}$. Thus we can apply Lemma 15 with $n = \prod_{p \in \mathcal{P}_1} p$ to get asymptotic uniformity (and independence) for all of these primes at once. From this we get $\Pr'(\text{some } p \in \mathcal{P}_1 \text{ divides } \delta_\ell) \rightarrow 1 - \frac{1}{\zeta(m)}$, via the Euler product formula for the zeta function. By Lemma A.1,

$$\Pr'(\text{some } p \in \mathcal{P}_1^c \text{ divides } \delta_\ell) < \sum_{p \notin \mathcal{P}_1} \frac{1}{p^m} \rightarrow 0,$$

where the inequality is just the sum-bound $\Pr(\cup_i E_i) \leq \sum_i \Pr(E_i)$ and it converges to zero as the tail of a convergent sequence. Lastly, $\Pr(\text{some entry is zero}) \rightarrow 0$ and the lemma follows. \square

Common divisors of random determinants. We now build up a series of lemmas regarding divisibility with respect to our partition of the primes of determinants of random matrices M_ℓ with columns independently distributed by \hat{A}_ℓ . We will refer to the upper left-hand $k \times k$ minor of such a matrix by $M_\ell^{(k)}$ (for $1 \leq k \leq m$).

Lemma A.4 (Divisibility of determinants by small primes). Let

$$\mathbf{P}_m(p) := 1 - \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{p^2}\right) \cdots \left(1 - \frac{1}{p^m}\right).$$

There exist constants $c_1, c_2 > 0$ such that for all ℓ, k , and $p < \ell^{\frac{1}{2}-\epsilon}$ (i.e., $p \in \mathcal{P}_1 \cup \mathcal{P}_2$),

$$\left| \Pr(p \mid d_\ell^{(k)}) - [\mathbf{P}_m(p)]^k \right| < c_1 e^{-c_2 \ell^{2\epsilon}}.$$

Furthermore,

$$\Pr(\text{no } p \in \mathcal{P}_1 \text{ divides } d_\ell^{(k)}) = \prod_{p \in \mathcal{P}_1} (1 - [\mathbf{P}_m(p)]^k) + c_1 e^{-c_2 \ell^{2\epsilon}}.$$

Proof. The number of nonsingular matrices with \mathbb{F}_p entries is

$$|GL_m(\mathbb{F}_p)| = (p^m - 1)(p^m - p) \cdots (p^m - p^{m-1})$$

out of p^{m^2} total matrices [13], so the ratio of singular matrices is $\mathbf{P}_m(p)$. Thus the lemma follows from the fact that each entry of M_ℓ approaches a uniform distribution with the error term decaying exponentially fast in ℓ . Summing the error over the km^2 entries appearing in k $m \times m$ matrices only worsens the constant c_2 that appeared in Lemma 15.

For the second statement we use the fact, noted in the last proof, that probabilities are asymptotically uniform/independent for all primes in \mathcal{P}_1 . The Chinese Remainder Theorem ensures that for any $m \times m$ matrices A with entries in $\mathbb{Z}/p\mathbb{Z}$ and B with entries in $\mathbb{Z}/q\mathbb{Z}$, there is a unique matrix C with entries in $\mathbb{Z}/pq\mathbb{Z}$ that agrees with both in the respective projections. Using this repeatedly, with $n = \prod_{p \in \mathcal{P}_1} p$, we count that the number of matrices over $\mathbb{Z}/n\mathbb{Z}$ such that no $p \in \mathcal{P}_1$ divides the determinant must equal $\prod_{p \in \mathcal{P}_1} |GL_m(\mathbb{F}_p)|$. The statement follows. \square

To get a similar bound for large primes, we prove two lemmas on the divisibility of the determinants of the submatrices $M_\ell^{(k)}$, and then combine them for a bound that works on \mathcal{P}_3 and \mathcal{P}_4 .

Lemma A.5 (Divisibility of determinants by large primes). For ϵ as above, there is a constant c such that for sufficiently large ℓ , any $1 \leq k \leq m$, and any prime $p \geq \ell^{1/2-\epsilon}$ (i.e., $p \in \mathcal{P}_3 \cup \mathcal{P}_4$), we have

$$\Pr'(\det M_\ell^{(k)} \equiv 0 \pmod{p}) < \frac{c}{\ell^{\frac{1}{2}-2\epsilon}} + \frac{c}{\sqrt{\ell}} + \frac{1}{p},$$

where \Pr' denotes conditional probability given that the matrix entries are nonzero. It follows that there is a constant c such that $\Pr'(p \mid \Delta_{\ell,i}) < c\ell^{2\epsilon-\frac{1}{2}}$ for $p \in \mathcal{P}_3 \cup \mathcal{P}_4$, and $\Pr'(p \mid \Delta_{\ell,i}) < cp^{\frac{4\epsilon-1}{2m+2}}$ for $p \in \mathcal{P}_3$.

Proof. For fixed m , we start with the $k = 1$ case and raise k one increment at a time to show that the probability that $M_\ell^{(k)}$ is divisible by p is $\frac{2(k-1)c}{\ell^{\frac{1}{2}-2\epsilon}} + \frac{(k-1)c}{\sqrt{\ell}} + \frac{1}{p}$. When $k = 1$, this follows from Lemma A.1.

Now suppose this is true for $M_\ell^{(k-1)}$. Introduce the equivalence relation $A \sim B \iff a_{ij} = b_{ij}$ for all $(i, j) \neq (k, k)$; that is, declare two $k \times k$ matrices equivalent if they agree in all entries except possibly the bottom right. Then there is a constant C_M for each matrix M such that

$$\det A = a_{kk} \det N + C_M \quad \forall A \in [M],$$

where N is the upper-left-hand $(k-1) \times (k-1)$ minor. Now if $p \nmid \det N$, then solving for a_{kk} gives $(\det A - C_M)(\det N)^{-1} \pmod{p}$, so at most $1/p$ of the a_{kk} values in \mathbb{Z} give a possible solution. Thus

there are at most $(2\ell^{1/2+\epsilon}/p) + 1$ matrices $A \in [M]$ with determinant divisible by p in this case, and since $\ell^{\frac{1}{2}-\epsilon} \leq p$ this has a conditional probability at most $(\frac{2\ell^{1/2+\epsilon}}{p} + 1)\frac{c}{\sqrt{\ell}} < \frac{2c}{\ell^{1/2-2\epsilon}} + \frac{c}{\sqrt{\ell}}$, given that the matrix falls in the equivalence class. (The estimate comes from multiplying the number of matrices by the probability upper-bound for each matrix; this bound is subject to an exponentially decaying error because the independence is only asymptotic, but that is dominated by the $\sqrt{\ell}$.)

By the $M_\ell^{(k-1)}$ hypothesis, the probability that $\det N$ is divisible by p is $< \frac{2(k-2)c}{\ell^{\frac{1}{2}-2\epsilon}} + \frac{(k-2)c}{\sqrt{\ell}} + \frac{1}{p}$, thus $\Pr'(\det M_\ell^{(k)} \equiv 0 \pmod{p}) < \frac{2(k-2)c}{\ell^{\frac{1}{2}-2\epsilon}} + \frac{(k-2)c}{\sqrt{\ell}} + \frac{1}{p} + \frac{2c}{\ell^{\frac{1}{2}-2\epsilon}} + \frac{c}{\sqrt{\ell}} = \frac{2(k-1)c}{\ell^{\frac{1}{2}-2\epsilon}} + \frac{(k-1)c}{\sqrt{\ell}} + \frac{1}{p}$. After enlarging c , the first statement follows for $M_\ell^{(k)}$. For the last statement, we want to combine these three terms. Since $p > \ell^{\frac{1}{2}-\epsilon}$, we first observe that $\frac{1}{p} < \frac{1}{\ell^{1/2-\epsilon}} < \frac{1}{\ell^{1/2-2\epsilon}}$, and clearly $\frac{1}{\sqrt{\ell}} < \frac{1}{\ell^{1/2-2\epsilon}}$ as well. Note that if $p \leq \ell^{m+1}$, then $\ell \geq p^{\frac{1}{m+1}}$, and we are done. \square

Lemma A.6 (Nonsingularity). $\overline{\Pr}(\Delta = 0) = 0$.

Proof. The idea is that determinant zero is a codimension-one condition. To show it rigorously, we prove the following stronger result: for fixed m , we will show that $\overline{\Pr}(\det M_\ell^{(k)} = 0) = 0$ for each $1 \leq k \leq m$. For $k = 1$, we note that $M_\ell^{(1)} = \hat{A}_{\ell,i}$, so the statement follows from Lemma A.2. Let's show that if it is true for $M_\ell^{(k-1)}$, then it is true for $M = M_\ell^{(k)}$. Let us write q_ℓ to denote the lower-right entry of $M_\ell^{(k)}$ and μ_ℓ to denote the list of the other $k^2 - 1$ entries $(M_{1,1}, \dots, M_{k,k-1})$. The induction hypothesis tells us the probability that $\det N = 0$ tends to zero for N the upper left-hand $k-1 \times k-1$ minor. Assuming that minor is nonsingular, there is exactly one value of q_ℓ making $\det M_\ell^{(k)} = 0$ for each μ ; call it $q(\mu)$. But, recalling that 0 is the most likely value for q_ℓ and that the different $\mu_\ell = \mu$ are disjoint events, we have

$$\Pr(\det M_\ell^{(k)} = 0) = \sum_{\mu} \Pr(q_\ell = q(\mu)) \leq \sum_{\mu} \Pr(q_\ell = 0) = \Pr(q_\ell = 0).$$

But q_ℓ is distributed like $\hat{A}_{\ell,i}$, so by Lemma A.2, this tends to zero. \square

Lemma A.7 (Lemma 35). Fixing m and any $k > 10m$, we have

$$\overline{\Pr}(d_\ell^{(k)} = 1) = \prod_{\text{primes } p} 1 - \left[1 - \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right) \cdots \left(1 - \frac{1}{p^m}\right)\right]^k.$$

Proof. We'll break down the probability by dividing the primes into the size ranges $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$, and \mathcal{P}_4 . As above, let $\mathbf{P}_m(p) := 1 - \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right) \cdots \left(1 - \frac{1}{p^m}\right)$, and note that $\mathbf{P}_m(p) \leq \frac{2^m}{p}$ because there are at most 2^m nonzero terms with denominators at least p . We clearly have the following bounds:

$$\begin{aligned} \Pr(p | d_\ell^{(k)} \text{ for some } p \in \mathcal{P}_1) &< \Pr(d_\ell^{(k)} > 1) < \Pr'(p | d_\ell^{(k)} \text{ for some } p \in \mathcal{P}_1) + \Pr'(p | d_\ell^{(k)} \text{ for some } p \in \mathcal{P}_2) \\ &\quad + \Pr'(p | d_\ell^{(k)} \text{ for some } p \in \mathcal{P}_3) + \Pr'(p | d_\ell^{(k)} \text{ for some } p \in \mathcal{P}_4) \\ &\quad + \Pr(\text{some entry is zero}). \end{aligned}$$

We apply Lemma A.4 and take a limit to get

$$\Pr(p | d_\ell^{(k)} \text{ for some } p \in \mathcal{P}_1) = 1 - \prod_{\mathcal{P}_1} \left(1 - [\mathbf{P}_m(p)]^k\right) + O(e^{-\ell^{2\epsilon}}) \longrightarrow 1 - \prod_{\text{primes } p} \left(1 - [\mathbf{P}_m(p)]^k\right).$$

We have thus shown that $\overline{\Pr}(d_\ell^{(k)} > 1) \geq 1 - \prod_{\text{primes } p} \left(1 - [\mathbf{P}_m(p)]^k\right)$, which implies that

$$\overline{\Pr}(d_\ell^{(k)} = 1) \leq \prod_{\text{primes } p} \left(1 - [\mathbf{P}_m(p)]^k\right).$$

Note that \Pr' conditions on an event whose probability tends to 1, thus $\lim_{\ell \rightarrow \infty} \Pr'(E) = \overline{\Pr}(E)$ if the limits exist.

To finish the theorem we must show the other four terms that bound $\Pr(d_\ell^{(k)} > 1)$ limit to zero, starting with the primes in \mathcal{P}_2 . We have

$$\Pr(p \mid d_\ell^{(k)} \text{ for some } p \in \mathcal{P}_2) < \sum_{\mathcal{P}_2} \Pr(p \mid d_\ell^{(k)}) = \sum_{\mathcal{P}_2} \left(\mathbf{P}_m(p) + O(e^{-\ell^{2\epsilon}}) \right)^k \longrightarrow 0,$$

where the $\mathbf{P}_m(p)$ term appears because $p < \ell^{\frac{1}{2}-\epsilon}$ means we can apply Lemma A.4. To justify the convergence to zero, recall that $\mathbf{P}_m(p) \leq \frac{2^m}{p}$ and $k \geq 2$.

We now handle the case of \mathcal{P}_3 , applying Lemma A.5 (and recalling that $k > 10m$ and $\epsilon < \frac{1}{10}$) to get

$$\Pr'(p \mid d_\ell^{(k)} \text{ for some } p \in \mathcal{P}_3) \leq \sum_{\mathcal{P}_3} \Pr'(p \mid d_\ell^{(k)}) = \sum_{\mathcal{P}_3} (\Pr'(p \mid \Delta_i)^k) \leq \sum_{\mathcal{P}_3} c \cdot p^{\frac{4\epsilon-1}{2m+2}k} \leq \sum_{\mathcal{P}_3} \frac{c}{p^2}.$$

Since the sum over all primes of p^{-2} converges, this tail certainly converges to zero as $\ell \rightarrow \infty$.

In the range \mathcal{P}_4 , since all coordinates of the random walk vector are $\leq \ell$, we have $|\Delta_\ell| \leq m!\ell^m < \ell^{m+1}$ for $\ell \gg 1$. Since $\Delta_\ell = 0$ is an asymptotically negligible event (Lemma A.6), we have

$$\Pr'(p \mid d_\ell^{(k)} \text{ for some } p \in \mathcal{P}_4) \longrightarrow 0,$$

because $\Pr(p \mid d_\ell^{(k)} \text{ for some } p \in \mathcal{P}_4) = \Pr(\Delta_{\ell,1} = \dots = \Delta_{\ell,k} = 0) \longrightarrow 0$, so $\Pr = \Pr'$. Finally, the probability of a zero entry also goes to zero (Lemma A.2), which completes the proof. \square